Spying on the Margins: The History, Law, and Practice of U.S. Surveillance Against Muslim, Black, and Immigrant Communities and Contemporary Strategies of Resistance

A Project South Report. Lead Author, Amith Gupta, Esq.
Edited by Azadeh Shahshahani and Manzoor Cheema

PROJECT SOUTH

Acknowledgments

Project South would like to thank the following people for their advice and assistance in making this report possible: Leena Al-Arian, Dr. Sami Al-Arian, Nicole Fauster, Mike German, Nadia Guzman, Bisan Hameed, Javeria Jamil, Hamid Khan, Zainab Khan, Lara Kiswani, Sabrine Mohamed, Celine Qussiny, Sue Udry, Elica Vafaie, Jeffrey Wang, Stephanie Guilloud, and Emery Wright.

Cover Page: Nahla Al-Arian, wife of Palestinian-American Muslim Professor Sami Al-Arian, shuffles through hundreds of CDs containing audio from the surveillance of all of her family's phone calls over a decade. (Halvorsen, Line. *USA vs. Al-Arian*. Exposed Film, 2007, vimeo.com/128413718.)

© Project South, February 2021

TABLE OF CONTENTS

INTRODUCTION 2

CHAPTER 1: THE HISTORY OF THE U.S. SURVEILLANCE STATE: ORIGINS TO THE 1990S 4

Defining Islamophobia 4
Islamophobia as Racism 4
The Trans-Atlantic Slave Trade & Muslims 5
Orientalism: Islam as Foreign and Dangerous 5
Modern Islamophobia 6
The Evolution of Surveillance 6
The Colonial and Racist Origins of Surveillance in the Americas 6
The Repression of The Labor Movement & The Surveillance State 6
U.S. Imperialism in the Philippines & The Surveillance State 8
The Repression of Dissent & Diversity: Early Twentieth Century Surveillance 9
The COINTELPRO Era 12
Reforms and their Limits 14
The Antiterrorism and Effective Death Penalty Act and Other Changes 15

CHAPTER 2: THE "WAR ON TERRORISM" AND THE CONTEMPORARY U.S.SURVEILLANCE STATE 15

Fearing Muslims: Preventative Policing & The "Radicalization" Thesis: 16
Invading Muslim Spaces: The Use of Informants, Ethno-Religious Mapping, and Entrapment 17
Brutalizing Muslims: Torture, Disappearances, Renditions, and Secret Detentions 18
Authorizing Torture and Secret Detentions 18
U.S. Torture of Detained People at GTMO and CIA Black Sites 19
Expanding Extraordinary Renditions 19
U.S. Torture in Iraq and Afghanistan Invasions 20
President Obama's Weak Reforms 21
Torture and Surveilling Muslims 21
Criminalizing Muslim Society: Prosecutions for "Material Support" 21
Programmatic Mass Surveillance 23
Authorizing Mass Surveillance: Statutes and Directives 23
Mass Surveillance in Practice 24
Leaks and Statutory Authorizations 26
The Call Detail Records Program 27
The Terrorist Surveillance Program and FISA Section 702 27
Federal and Local Surveillance Collaboration 28
Some Reforms 29
Watching Muslims 29
The Trump Era 30
"Black Identity Extremism" and the Repression of Black Resistance 30
Banning Muslims 30
Surveilling Anti-Deportation Efforts 31
FISA Limits 31

CHAPTER 3: CHAPTER 3: THE LEGAL CONTOURS OF U.S. FEDERAL LAW ON SURVEILLANCE AND RELATED LITIGATION 32

First Amendment Challenges to Surveillance 32
The Laird Barrier 32
Overcoming Laird 33
The First Amendment and Material Support Prosecutions 34
Fourth Amendment Challenges to Surveillance 34
A Reasonable Expectation of Privacy 34
The Third Party Doctrine 36
The Foreign Intelligence Surveillance Exception 36
The Border Search Exception 37
Ethno-Religious Profiling as Probable Cause 37
Equal Protection Claims Under the Fourteenth and Fifth Amendments 38
Intentional Discrimination 38
Discriminatory Application of Facially Neutral Laws 39
The State Secrets Hurdle 39

CHAPTER 4: SURVEILLANCE BY STATE 40

GEORGIA 42
Expansive Surveillance Guidelines at the Georgia Bureau of Investigation & GISAC Fusion Center 42
Directive 7-6: Overarching Intelligence Gathering Guidelines 42
Directive 8-6-5: Social Media Guidelines 43
Directive 8-8-23: Facial Recognition Software Guidelines 43
Annual Privacy Presentations 43
Privacy Audits 43
Conclusions about GBI & GISAC 44
Federal-to-Local Spying and Prosecution 44
JTTF & Pentagon Monitoring Protest Activity 44
Preemptive Prosecutions of Shifa Sadequee & Syed Harris Ahmed 44
Recent Incidents 45
NORTH CAROLINA 46
Expansive Surveillance Guidelines at the State Bureau of Investigation & NCISAAC 46
Federal-to-Local Spying and Prosecution 47
The JTTF-led Targeting and Prosecution of the Raleigh 7 47
Recent Incidents 48
FLORIDA 48
Fusion Centers: SEFFC and the Florida Fusion Center 48
Federal-to-Local Spying and Prosecution 48
Fusion Centers and JTTF Target Muslim Teens 48
The Collapse of the FISA Wall: The Prosecution of Sami Al-Arian 49
Targeting Black Muslim Poverty: The Liberty City 7 50
LOUISIANA 51
Expansive Surveillance Guidelines at LA-SAFE 51
Federal-to-Local Spying and the Climate of Fear 51
SOUTH CAROLINA 51
Expansive Surveillance Guidelines at SCIIC and in Local Police Departments 51
The Charleston Police Department 51

CHAPTER 5: COMMUNITIES RESIST SURVEILLANCE 52

Obstacles and Limits to Traditional Strategies 53
Litigation 53
Statutory Changes 55
Reclaiming Muslim Community Spaces in Atlanta, GA and Kenner, LA 55
Shutting Down CVE Programs in Los Angeles, CA 56
Ending JTTF Agreements in San Francisco, CA 57
Halting the Expansion of Fusion Centers in Georgia 58

CONCLUSION & RECOMMENDATIONS 61

APPENDIX 62 - 79

INTRODUCTION

In the aftermath of September 11th, 2001, Project South worked with our regional movement partner Highlander Research & Education Center to hold an emergency meeting for movement leaders from across the U.S. South. As a Southern-based movement organization rooted in the Black Radical Traditions of the U.S. South, we anticipated that the events of September 11th and the State response would create a paradigm shift for the social, economic, and political conditions in our country. As a result of that meeting, Project South initiated a set of popular education workshops in 2002 and published a workbook called Roots of Terror to provide historical context for the "War on Terror" and USA PATRIOT Act after 9/11. Since that time, Project South has developed analysis and programs to contend with the rise in Islamophobia as a critical frontline in the work for racial justice and movement building. In 2009, Project South's organizing efforts supported the family of Shifa Sadequee, a member of our community. Sadequee, a young Muslim man in Atlanta, was targeted, surveilled, kidnapped in Bangladesh, charged, and convicted in a U.S. federal court on four counts of terrorism. The case (explored in more depth in Chapter Four) exposed the lengths to which preemptive prosecution and social control mechanisms had evolved, and the organization continued to monitor and organize around state social control. A 2011 People's Movement Assembly connected the impacts of the U.S. War on Drugs, War on Immigrants, and War on Terror on Black, Brown, and Muslim communities. Project South launched a more cohesive set of legal and advocacy programs led by attorney Azadeh Shahshahani in 2015.

In 2018, Project South developed a more concentrated effort to document state surveillance practices targeting Muslim, Black, and immigrant communities. A number of developments informed the project: the continued expansion and normalization of mass surveillance in U.S. society; the elevation of Islamophobia to the highest level of U.S. Executive power; and the targeting of people for surveillance, primarily consisting of individuals from Muslim, immigrant, and/or African American backgrounds. Project South's Protect and Defend Initiative received repeated reports from members of local Muslim communities in the U.S. South about unwelcome visits from law enforcement and suspicion that various law enforcement agents were engaged in discriminatory surveillance. Beginning in 2019, Project South's Protect and Defend Initiative began an extensive effort to build our legal and historical knowledge of surveillance policies; obtain available information from policing agencies at the municipal, state, and federal levels about existing surveillance policies; and reach out to Muslim communities throughout the U.S. South to document suspected state surveillance. This report is an initial product of those ongoing efforts.

This report aims to summarize the specific history, politics, and legal backdrop of Islamophobia and surveillance in the United States and the goals that they serve; lay out the existing framework through which they work, including federal, state, and municipal surveillance programs we have documented throughout five states in the U.S. South; highlight the impact of these policies on Muslim communities using data from Project South surveys and statements of community members who have spoken with Project South; and, finally, suggest strategies for moving forward based on what has worked.

The first chapter traces the origins of Islamophobia as a form of anti-Black racism connected to the trans-Atlantic slave trade. The report connects the rise of the surveillance state to crush social movements and extreme forms of surveillance and repression that emerged in the 1960s, like COINTELPRO, and continued into the 1990s, leading up to the 9/11 attacks. Chapter Two describes the shift towards more significant surveillance and "counter-terrorism" programs justified by President George W. Bush's War on Terror. The efforts included mass round-ups of Muslims, preventative policing, and entrapment, all of which have shaped the surveillance state for African American and immigrant communities throughout the twenty-first century.

Chapter Three investigates the legal precedents of federal law as it relates to surveillance and potential challenges communities can consider. The fourth chapter dives into specific surveillance and social control regulations in Georgia, North Carolina, Florida, Louisiana, and South Carolina, detailing specific case study examples in each. The fifth chapter explores resistance strategies to contend with the surveillance state. From litigation to community organizing and education efforts, the report provides possible avenues and several successful examples of challenging anti-Muslim ordinances and Joint Terrorism Task Force initiatives. Project South's organizing to stop SB15—a Georgia Senate Bill that would have expanded data mining, surveillance, and policing into high schools, targeting African American and immigrant youth—is discussed in depth as an example of combining legal, legislative, and organizing strategies to win.

This report offers a historical and legal perspective to support movement organizing that aims to dismantle surveillance policies and practices as part of a wider call for the abolition of prisons, police, and law enforcement agencies that spy on our communities. It is our hope that the report provides tools and insights that are helpful to our collaborative efforts to eliminate social control efforts by federal, state, and local agencies.

Content Warning: Note that a brief section of Chapter 2 of this report discusses the use of torture in depth, and some of the content is disturbing and involves sexual violence.

"This report offers a historical and legal perspective to support movement organizing that aims to dismantle surveillance policies and practices as part of a wider call for the abolition of prisons, police, and law enforcement agencies that spy on our communities."

CHAPTER 1

THE HISTORY OF ISLAMOPHOBIA WITHIN THE U.S. SURVEILLANCE STATE: ORIGINS TO THE 1990S

DEFINING ISLAMOPHOBIA

Islamophobia as Racism

Islamophobia is often erroneously reduced to a form of religious discrimination. In fact, Islamophobia is a form of racism with a lengthy historical pedigree. That is, while Islamophobia often takes the form of religious discrimination, it is an ideology that encompasses a number of assumptions about the identity of individuals perceived to be associated with Islam or Muslim communities.

The Trans-Atlantic Slave Trade & Muslims

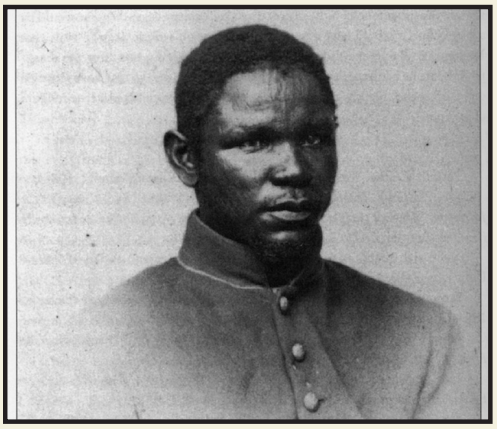
Islamophobia as a form of racism was institutionalized in the earliest days of the United States and is intimately linked to European colonialism and the trans-Atlantic slave trade. As early as the sixteenth century, slave trading states seeking to protect the institution of slavery from rebellion issued restrictions on the trade of enslaved African Muslims based on the contention that Islamic teachings – not the barbarism of slavery – were responsible for rebellions by enslaved people.[1] Europeans relied on Orientalist tropes of Islamic savagery and irrationality growing from Europe's colonial warfare against the Ottoman Empire to crafted lurid tales in which Islam was an innately "foreign" and dangerous identity.[2] Despite the widespread presence of Islam throughout the world, these European conceptions of Islam naturalized Islam as an identity to certain parts of the world and attached to it signifiers of "danger" and rebellion. The earliest Muslim communities in the Americas were brought as enslaved Africans from Senegambia in West Africa to what would become the thirteen American colonies. Having higher literacy rates than many non-enslaved European settlers, some enslaved Muslims became highly influential in society. Several, like Abdul Rahman Ibrahima, played an important role in white business and political circles as advocates of abolitionism.[3]

Right: Abdul Rahman Ibrahima was born in Timbo, present-day Guinea, before being enslaved and brought against his will to Mississippi (Abdul Rahman, 1828, by Henry Inman, 1828. From the Colonization and Journal of Freedom, 1834, frontispiece.). In addition to holding places of significant influence in spite of their enslavement, enslaved Muslims like Omar Ibn Sayyid and Nicholas Said advocated against or actively fought to end slavery.[4]

1 Andrew Lawler, Muslims Were Banned From the Americas as Early as the 16th Century, SMITHSONIAN, February 7, 2017, https://www.smithsonianmag.com/history/muslims-were-banned-americas-early-16th-century-180962059/.

2 Deepa Kumar, ISLAMOPHOBIA AND THE POLITICS OF EMPIRE, Ch. 2 (2012).

3 Edward E. Curtis, The Black Muslim Scare of the Twentieth Century, ISLAMOPHOBIA IN AMERICA 75, 78-84.



Above:Nicholas Said, circa 1863-1866, Carte de visite, photograph number 70.93, Massachusetts Historical Society.

Notably, early enslaved Africans like Ibrahima were often erroneously described by both their supporters and captors as Mediterranean rather than sub-Saharan African. These assumptions were premised both on the racist notion that Black Africans could not be intelligent and dignified, and on the assumptions of Islam as a particular "foreign" identity associated with the Mediterranean. Abolitionists, despite their opposition to slavery, often sought to repatriate enslaved people to West Africa on the premise that their identity – not their enslavement – was out of place in America, and therefore emphasized stereotypes of foreignness that they associated with Ibrahima's practice of Islam.[5]

Below:Omar Ibn Sayyid wrote extensively in Arabic and English about the injustices of slavery after human traffickers kidnapped him from Futa Toro in present-day Senegal and took him against his will to North Carolina to be enslaved (R. L. Simpson Af.-Am. Collection)Orientalism: Islam as Foreign and Dangerous

The belief that Islam was fundamentally foreign and dangerous characterized even the earliest period of U.S. history. The nation's first immigration law, the Naturalization Act of 1790, barred citizenship to a number of different communities, including "Muslims," a designation that was presumptively applied to all Middle Eastern immigrants of any faith.[6] On some level, these stereotypes and misguided readings of Islam inherited from Europe would continue to characterize the racism that the U.S. government would direct toward Muslims of all backgrounds, including but not limited to Black people.

By the early twentieth century, a fledgling U.S. surveillance state had coded both Black Muslims descended from enslaved communities and other immigrant Muslims as communities that were particularly prone to "radicalism." Adopting the rhetoric of racialization that continues to characterize present-day Islamophobia, intelligence agencies produced materials and documentation suggesting that legitimate expressions of Islamic identity were limited to religious practice, thereby differentiating the mere practice of Islamic customs from supposed "radicalism" emanating from Muslim community organizing and political advocacy. These fears closely tailed the U.S. state's increasing nativism and fears of Black rebellion in the aftermath of World War I. While interconnected, diverse, multi-sect communities of Muslims from immigrant and African American backgrounds began to thrive in the early twentieth century, government repression and anti-immigrant legislation negatively impacted these communities. "Islam" and "Muslim" simply became identifiers of "danger" that the U.S. government associated with those who agitated for social change.[7]

By the 1940s, the U.S. government would open investigations into Black Muslim communities that it suspected, without any basis, of collaboration with Imperial Japan. In the ensuing years, Black Muslim organizations, including the Nation of Islam, became some of the most prominent targets of FBI surveillance and repression. The age of limited surveillance reforms that followed the FBI's notorious domestic political spying program, COINTELPRO, did not result in any limitations on the Islamophobia of the U.S. surveillance state. Rather, the 1970s and 1980s brought the rise of the neoconservative movement, strong reactions to the Iranian hostage crisis, and a newly constructed, particularly "brown" Islamic "threat" that challenged U.S. foreign policy in the Middle East.[8]

Modern Islamophobia

In the aftermath of the 1993 World Trade Center Bombing and the climate of fear prompted by the Oklahoma City Bombing (which was not carried out by Muslims), the federal government aggressively rolled back existing limits on the government's ability to surveil and deport people, often from Muslim-majority countries. But it was during the aftermath of the September 11th attacks in 2001 that the lengthy history of Islamophobia in the U.S. took on particularly extreme forms. In the immediate aftermath of the attacks, the U.S. government aggressively rounded up hundreds of Muslim immigrants based on minimal or non-existent visa irregularities and jailed, physically abused, and deported many of them.[9] In addition, the FBI and other intelligence agencies were able to drastically expand the scope of their power through legal changes that

---

4 William Costel Tamplin, Who Was 'Umar ibn Sayyid? A Critical Reevaluation of the Translations and Interpretations of the Life, J. ARABIC AND ISLAMIC STUDIES 125 (2016); Safet Dabovic, Out of Place: The Travels of Nicholas Said, CRITICISM 59 (2012).
5 Id.
6 Mariam Elba, How Islamophobia was Ingrained in America's Legal System Long Before the War on Terror, THE INTERCEPT (May 6, 2018); Khaled Beydoun, 'Muslim Bans and the (Re)Making of Political Islamophobia, 2017.5 ILL. L. R. 1734 (2017).
7 Curtis, supra note 3 at 84.
8 Kumar, supra note 2 at Ch. 7.
9 Office of the Inspector General of the U.S. Department of Justice, The September 11 Detainees: A Review of the Treatment of Aliens held on Immigration Charges in Connection with the Investigation of the September 11 Attacks (2003).

enabled religious and racial discrimination and violence. Narratives of Islamic radicalism were developed by local and federal agencies to justify expansive "security" policies based on racism, including immigration restrictions and aggressive foreign policy endeavors. All of these policies were directly or indirectly tied to a massive expansion in surveillance efforts by all levels of government.

The Evolution of Surveillance

The Colonial and Racist Origins of Surveillance in the Americas

The U.S. government's mapping and ordering of both land and the people inhabiting it trace back to the Western settlement of the Americas. In the process of "discovering" new lands, European settlers sought to bring order to the "wilderness" they encountered by mapping the land and its indigenous inhabitants. Traders and missionaries carried out some of the earliest systematic attempts to order and map out knowledge about indigenous "others," which were eventually formalized through colonial bureaucracies such as the Office of Indian Affairs, and the later Bureau of Indian Affairs.[10] The simultaneous settlement of the land and institutionalization of slavery established non-white race groups as "others" which in turn informed identification practices of early slave patrols.[11]

Surveillance is arguably inherent in various forms of colonialism and racism, including slavery and the development of Jim Crow Apartheid. Still, the process by which these early forms of surveillance developed into the modern surveillance state in the late nineteenth and early twentieth century also grew from two particular historical developments: the repression of the industrial labor movement and U.S. imperialism in the Philippines.

The Repression of the Labor Movement & The Surveillance State

In the aftermath of the Civil War, one of the first private police agencies to receive a contract from the federal government for the enforcement of federal law was the agency of Allan Pinkerton, whose agents were known as Pinkertons.[12] Having served the security needs of various high-profile clientele, including President Abraham Lincoln, the Pinkerton agency became notorious not only for protecting banks and railroads from attempted robberies but also for detecting and disrupting industrial labor organizing.

Alongside the Pinkertons' involvement in notorious massacres of organized labor during the late nineteenth and early twentieth centuries, the Pinkertons used federal funding to hone and craft the skills of surveilling union organizing in company towns. In the process of doing so, the Pinkertons not only construed a wide variety of civilian practices, such as labor organizing, to be indicative of or equivalent to law-breaking, but also utilized infiltration, agents provocateur, and violence to forcefully repress the labor movement. Pinkertons painted the movement as a bastion of violent radicalism, often based on little to no credible evidence.

By the early twentieth century, infiltration into the labor movement had become a common practice in U.S. industry.[13] While strike-breaking was one particularly destructive tactic of the Pinkertons, the agency incurred much of its profits from surveillance of labor organizations alone. Though the Pinkertons were not the only private agency responsible for surveilling and disrupting organized labor through these tactics, they remain one of the most notorious. While the agency limited its involvement in strike-breaking in the aftermath of the passage of the Wagner Act of 1937, the agency continued marketing its role in industrial "security." By the time of the creation and expansion of the FBI, which largely took over the process of enforcing domestic federal law on behalf of the Department of Justice, many Pinkerton tactics, methods, and personnel had been incorporated into federal practice, including the use of security indexing, fingerprinting, criminalizing political dissent, and the use of informants and agents provocateur. This would become clear during the First World War, its immediate aftermath, and the COINTELPRO period that followed.

U.S. Imperialism in the Philippines & The Surveillance State

Another underrecognized development in the creation of the modern U.S. surveillance state was the U.S. imperial occupation of the Philippines. Beginning with the Spanish-American War in 1898, the United States began its foray into modern imperial control of territory beyond its continental borders. With the conquest of Manila Bay on May 1, 1898, the United States had officially become an imperial power. While the United States began the invasion under the pretense of supporting Filipinos in their struggle against imperial Spain, within months, the United States had complete control of the Philippines and quickly became an occupying army, just as the U.S. invaded, occupied, and initiated colonization of Puerto Rico and Guam at this same time.

In his seminal study on U.S. pacification of the Filipino resistance and the construction of a then- unprecedented surveillance state to accomplish this task, historian Alfred McCoy concludes that U.S. surveillance in the Philippines was fundamental to the construction of a domestic surveillance state in the United States. This process was established by using the Philippines as a sort of "laboratory" for surveillance tactics that could not be pursued against U.S.

10 Arun Kundnani & Deepa Kumar, Race, surveillance, and empire, INT'L SOCIALIST REV. 96:3 (2015).
11 Id. at 4.
12 Ward Churchill, From the Pinkertons to the PATRIOT Act: The Trajectory of Political Policing in the United States, 1870 to the Present, 4 CR: THE NEW CENTENNIAL REVIEW 1, 3 (2004).
13 Id. at 16-17.

"By restricting constitutional protections and creating a new "terrorism" statutory framework criminalizing extremely broad categories of conduct, the FBI regained significant authority to target Muslim, Black, and immigrant communities for surveillance and investigation."

Detroit Publishing Co, P., Hart, E. H., photographer. American troops on ramparts at Manila. Philippines Manila, None. [Between 1898 and 1901] [Photograph] Retrieved from the Library of Congress, https://www.loc.gov/item/2016804829/.

citizens without potentially running afoul of the law, including many of the tactics that would subsequently be employed domestically, while training military and police personnel on how to spy on communities that they viewed as "subversive."[14] Specifically, McCoy writes:

> In building a U.S. intelligence capacity, empire's stamp on the nascent national security apparatus was both broad and deep, from data management to larger design. In both colonial Manila and wartime Washington, counterintelligence was characterized by similarities large and small. The reduction of voluminous amounts of information to a single card for every subject. Recruitment of civilian auxiliaries whose identities were concealed by numbered codes. Covert operational procedures for surveillance and infiltration. An ethnic or racial template for the perception of threat. Mass relocation of suspect populations. The systematic use of scandal as political disinformation. And, above all, a sense of omnipotence over peoples deemed alien and therefore lesser.[15]

The Repression of Dissent & Diversity: Early Twentieth Century Surveillance

In 1908, President Theodore Roosevelt and Attorney General Charles Bonaparte created the Bureau of Investigation without consulting Congress. In the earliest years of the Bureau, few crimes fell under purely federal jurisdiction. From the beginning, the Bureau targeted racial and ethnic minorities and political subversives, utilizing the tactics and methods that had been developed in part through the imperial occupation of the Philippines and the contemporaneous efforts to crush the labor movement.[16]

Though other intelligence agencies such as the Office of Naval Intelligence and the Military Intelligence Division were in existence at the start of the First World War, it was the Bureau whose capacity would rapidly increase during the lead up to the U.S.'s entry into the war in 1917. The Bureau had already been targeting suspected allies of Germany despite the country's official neutrality in the war. The federal government aggressively escalated its campaign against peace activists and other dissenters upon official entry into the war.[17]

In 1917, Congress passed the Espionage Act, which criminalized the publication of anti-war advocacy or "false statements" intended to promote the opposing side of the war and even empowered the Postmaster to seize mail materials that they determined to fit these categories. The following year, Congress passed the Sedition Act which criminalized expressions of disloyalty to the U.S. war effort. Investigating these acts, the Bureau of Investigation carried out the kinds of operations that continue to characterize much of its investigative behavior in the twenty-first century—such as intimidating visits to antiwar activists to deter them from speaking out and infiltration through undercover informants—in order to implement the overtly political sedition laws of the era.[18] The Bureau treated involvement in pacifist, socialist, or leftist movements as well as race and immigration status as proxies for "disloyalty."[19]

---

14 - 19 See Appendix

It was after the war that the Bureau carried out one of its most egregious abuses. In response to a series of anarchist bombings, including one that targeted Attorney General A. Mitchell Palmer, the Bureau's General Intelligence Division, originally known as its "Radical" Division, carried out a series of raids across the country. Led by a young J. Edgar Hoover, the Palmer Raids culminated in the violent arrests of some six thousand people, many of them immigrants, based solely on their political activities and immigration status. Thousands were subsequently deported.[20] Though the raids led to considerable backlash and prompted public support for reining in the Bureau, Hoover's political policing continued for several years amid significant public controversy. This included the Bureau's decision to spy on members of Congress over their opposition to the Hoover Administration during the Teapot Dome Scandal, one of several corruption scandals that led the Administration's popularity to collapse.[21]

In 1924, President Calvin Coolidge's Attorney General, Harlan Fiske Stone, attempted to abolish the General Intelligence Division and limit the Bureau's activities to the investigation of specific crimes after the ACLU documented a series of the aforementioned abuses and showed them to Stone. Hoover elided these limits by simply preserving his "Official and Confidential" Intelligence files to continue domestic espionage covertly, including against the ACLU, and by finding alternative statutory justifications for continuing to spy.[22] Hoover had also begun surveilling his political opponents, including the Secretary of Labor who exercised his authority to dismiss many of the deportation cases against targets of the Palmer Raids.[23] As such, despite public outcry and opposition from within the federal government, the Bureau continued to carry out broad and politically-motivated intelligence activities while maintaining security indexes on those it viewed with suspicion including Black American intellectual and leader Marcus Garvey[24]. Notably, based on the Supreme Court's 1928 ruling in Olmstead, the Bureau was able to engage in wiretapping without running afoul of the law.[25]

Below: The I.W.W. (International Workers of the World) New York City headquarters after Palmer Raid, 1919. Credit: Courtesy of the Labadie Collection, University of Michigan.

While leftist movements preoccupied much of the Bureau's interwar efforts, the climate of social unrest and mobilization toward class and racial equality that characterized the immediate aftermath of the First World War also prompted the Bureau to target immigrant communities and people of color. A particular target during this period was the increasingly diverse Muslim community throughout the United States. In addition to surveilling both Muslim and non-Muslim Black organizations, the Bureau feared the increasing intercommunal organizing of Muslim communities across sects and nationalities and coded Muslims as potential threats. By the early 1930s, the FBI was targeting Black Muslim-influenced organizations such as the Moorish Science Temple.[26]
With the beginning of World War II in Europe, President Franklin Delano Roosevelt directed Hoover to investigate pro-Nazi organizations alongside the perennial Communist threat that the federal government perceived among all dissidents. In 1935, the Bureau was reorganized as the Federal Bureau of Investigation (FBI), with Hoover as director. FDR called on Hoover to officially resume domestic espionage in 1936, and expanded the FBI's authority in 1939, alongside directing the Office of Naval Intelligence and the Military Intelligence Division to track "subversives."[27]

During World War II, the FBI spied on a number of immigrant communities and investigated Japanese-American leaders before and during Japanese internment. It was also charged with pursuing any Japanese-Americans who escaped the internment camps.[28] The FBI's RACON investigation in particular targeted Black Muslim groups perceived as disloyal to the United States and supportive of Japan. Documents detailing the RACON investigation make clear that the FBI viewed Muslim communities with deep suspicion, often distinguishing between what the FBI perceived as legitimate expressions of religious belief, limited to prayer, and those it perceived as "subversive," namely those suggesting community organizing and political engagement.[29]

The COINTELPRO Era

The aftermath of World War II and the beginning of the Cold War saw the creation of additional intelligence gathering organizations and programs. The National Security Act of 1947 created the Central Intelligence Agency, and a National Security Intelligence Directive in 1952 created the National Security Agency. By the mid-1970s, the world would learn that like the FBI, these agencies engaged in aggressive and covert domestic espionage.

---

20 - 29 See Appendix

But it was the FBI's 1956 COINTELPRO, or Counter-Intelligence Program, whose expansiveness, politicization, and egregiousness earned unbridled notoriety. The program was exposed to the public by a group of peace activists who broke into an FBI office in 1971 and uncovered evidence of it, prompting a series of extensive Senate investigations led by Frank Church. These investigations detailed both the program and the entire history of domestic spying by the FBI, CIA, NSA, and the military. Summarizing its findings, the Church Committee wrote:

> The Government has often undertaken the secret surveillance of citizens on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts on behalf of a hostile foreign power. The Government, operating primarily through secret informants, but also using other intrusive techniques such as wiretaps, microphone "bugs", surreptitious mail opening, and break-ins, has swept in vast amounts of information about the personal lives, views, and associations of American citizens. Investigations of groups deemed potentially dangerous-and even of groups suspected of associating with potentially dangerous organizations-have continued for decades, despite the fact that those groups did not engage in unlawful activity. Groups and individuals have been harassed and disrupted because of their political views and their lifestyles. Investigations have been based upon vague standards whose breadth made excessive collection inevitable. Unsavory and vicious tactics have been employed-including anonymous attempts to break up marriages, disrupt meetings, ostracize persons from their professions, and provoke target groups into rivalries that might result in deaths. Intelligence agencies have served the political and personal objectives of presidents and other high officials. While the agencies often committed excesses in response to pressure from high officials in the Executive branch and Congress, they also occasionally initiated improper activities and then concealed them from officials whom they had a duty to inform. [30]

Discussing the breadth of the number of people affected by COINTELPRO and other domestic spying programs of the time by the CIA and the NSA, the Committee summarized:

> Nearly a quarter of a million first class letters were opened and photographed in the United States by the CIA between 1953-1973, producing a CIA computerized index of nearly one and one-half million names. At least 130,000 first class letters were opened and photographed by the FBI between 1940-1966 in eight U.S. cities.' Some 300,000 individuals were indexed in a CIA computer system and separate files were created on approximately 7,200 Americans and over 100 domestic groups during the course of CIA's Operation CHAOS (1967-1973). Millions of private telegrams sent from, to, or through the United States were obtained by the National Security Agency from 1947 to 1975 under a secret 'arrangement with three United States telegraph companies.
>
> An estimated 100,000 Americans were the subjects of United States Army intelligence files created between the mid-1960's and 1971. Intelligence files on more than 11,000 individuals and groups were created by the Internal Revenue Service between 1969 and 1973 and tax investigations were started on the basis of political rather than tax criteria.' At least 26,000 individuals were at one point catalogued on an FBI list of persons to be rounded up in the event of a "national emergency".[31]

Credit: Malakhi Helel is licensed under CC BY-ND 2.0)

---

30 Staff of the S. Select Comm. to Study Governmental Operations with respect to Intelligence Activities, 94th Cong., Report on Intelligence Activities and the Rights of Americans, Book 2, 5.
31 Id. at 6-7.

Regarding the Army, the report summarized both the expansive infiltration, systematic documentation and "questionable tactics" of the Army's domestic surveillance program from 1968 to 1970, ostensibly to manage "civil disturbances" involving Black rebellions throughout U.S. cities:

> About 1500 Army intelligence agents were engaged in monitoring civilian protests in 1968. These agents routinely monitored civilian political activities in the communities to which they were assigned, and occasionally were used as part of concerted intelligence operations undertaken by the Army during the major political protests of the late 1960s…
> …Army agents covertly penetrated the organizational structure of civilian political groups, attended their meetings, and participated in their private and public activities. They also were inserted into public demonstrations of all dimensions [including]…the Poor Peoples' March to Washington in April, 1968…protests of a welfare mothers organization in Milwaukee, Wisconsin…a coalition of church youth groups in Colorado Springs, Colorado…antiwar groups in Chicago…[and] a Halloween party for elementary school children in Washington, D.C., where they suspected a local "dissident" might be present…Army agents posed as students to monitor classes in "Black Studies" at New York University, where James Farmer, former head of the Congress on Racial Equality, was teaching…
> …Army intelligence agents frequently posed as newsmen in order to photograph and interview "dissident" personalities. Photographing participants in political activities itself became a widely used intelligence technique…Army agents generally refrained from aggressive activities against civilian protestors, but occasionally they engaged in conduct designed to harass or confuse such groups.
> …In all, the Army probably maintained files on at least 100,000 Americans from 1967 until 1970. Among them were: Dr. Martin Luther King, Jr., Whitney Young, Julius Hobson, Julian Bond, Arlo Guthrie, Joan Baez, Major General Edwin Walker, Jesse Jackson, Walter Fauntroy Dr. Benjamin Spock Rev William Sloane Coffin, Congressman Abner Mikva, Senator Adlai Stevenson as well as clergymen, teachers, journalists, editors, attorneys, industrialists, a laborer, a construction worker, railroad engineers, a postal clerk, a taxi driver, a chiropractor, a doctor, a chemist, an economist, a historian, a playwright, an accountant an entertainer, professors, a radio announcer, business executives, and authors" who became subjects of Army files simply because of their participation in political protests of one sort or another. In addition, one witness told the Ervin subcommittee that "it was no exaggeration to state that (the Army's files) covered virtually every group engaged in dissent in the United States."[32]

Specific COINTELPRO tactics used by the FBI that the Committee mentioned included:

- Anonymously attacking the political beliefs of targets in order to induce their employers to fire them;
- Anonymously mailing letters to the spouses of intelligence targets for the purpose of destroying their marriages;
- Obtaining from IRS the tax returns of a target and then attempting to provoke an IRS investigation for the express purpose of deterring a protest leader from attending the Democratic National Convention;
- Falsely and anonymously labeling as Government informants members of groups known to be violent, thereby exposing the falsely labelled member to expulsion or physical attack;
- Pursuant to instructions to use "misinformation" to disrupt demonstrations, employing such means as broadcasting fake orders on the same citizens band radio frequency used by demonstration marshals to attempt to control demonstrations and duplicating and falsely filling out forms soliciting housing for persons coming to a demonstration, thereby causing "long and useless journeys to locate these addresses.[33]

---

32 Id. at Book 3, 800-804.
33 Id.

The Committee noted several particularly egregious acts carried out by the FBI. These included providing surveillance information to the Chicago Police Department that aided in that Department's raid of a Black Panther Party apartment and the ensuing execution of Black Panther Party activists Fred Hampton and Mark Clark.[34] These acts were the result of a coordinated and aggressive campaign to destroy the Black Panther Party altogether.[35] FBI agents specifically cited the political speeches of Black Panther Party activists Stokely Carmichael and H. Rap Brown (known today as Imam Jamil Al-Amin) as evidence of the need for surveillance and as a model of political views and speech that generally ought to be the target of surveillance.[36]

Above: Chicago police remove the body of Fred Hampton, leader of the Illinois Black Panther party, who was slain in a gun battle with police on Chicago's west side, December 4, 1969. Shooting erupted as police arrived at a building next to Black Panther offices to serve a warrant. (AP Photo/ Wilfredo Lee)

The report documented the FBI's wiretapping of Martin Luther King. Jr. on the grounds that he might be a "Communist Sympathizer," along with efforts to use intimate details of his life to ruin his marriage and blackmail him into committing suicide.[37] The report also castigated the FBI for investigating the NAACP over the course of decades despite the Bureau's acknowledgment that the organization was not involved in Communist activities.[38]

The report similarly documented the extremism of the COINTELPRO efforts against dissident movements more generally. Specifically, the FBI opened investigations into every student member of Students for a Democratic Society and every Black Student Union member irrespective of any potentially criminal activity for the purpose of screening individuals who applied for government jobs.[39] The FBI attempted to destroy the young radicals and changemakers (disproportionately Black and people of color) by publishing negative photographs of activists, informing students' parents of their political activities, and using "misinformation" to falsely notify members that events had been cancelled.[40] The FBI directed every field office to investigate every public university as a hotbed of potential subversive influence.[41] COINTELPRO also continued an even longer investigation that involved the disruption, burglary, and sabotage of the Socialist Workers Party since the 1930s.[42] The report similarly notes that the FBI gathered the names and political opinions of every individual in the Women's Liberation Movement.[43]

In the course of spying on dissenters, the FBI had also targeted the Nation of Islam, continuing the tradition of viewing Muslims generally and Black Muslims particularly as subversive threats to the social order. The FBI spread derogatory information about local NOI chapters to portray them as "violent" even when the Bureau knew this was untrue, and wiretapped the organization's offices even after the authorizations for wiretapping had expired and where the Bureau conceded that there was no evidence of criminal wrongdoing.[44]

Reforms and Their Limits

The exposure of COINTELPRO and other domestic intelligence gathering programs, as well as the Watergate scandal, prompted significant but limited changes in all branches of the government. Although some of these changes placed important limits on the ability of intelligence agencies to spy on the public, others turned out to be ineffective at restraining intelligence agencies.

First, Congressional Intelligence Committees were established in 1976 and 1977 to provide oversight of intelligence agencies. These committees could theoretically issue budgetary restrictions on the FBI and other intelligence agencies, though the extent of their effectiveness is limited by secrecy: for example, much of the FBI's budgetary information is kept secret, and Congress itself has limited access to information about ongoing investigations.[45]

To stave off a Congressional charter that would regulate the FBI, Attorney General Edward Levi issued guidelines to the FBI's domestic intelligence investigations which delineated when and under what circumstances the FBI could open investigations. Under the Levi Guidelines, the FBI would need a criminal nexus in order to initiate an investigation. That is, officers needed the "possibility" of criminal activity to open a limited preliminary inquiry as well as "specific and articulable facts" that the targets of investigation were violating criminal law in order to open a full investigation.[46] An additional set of guidelines limited the use of confidential informants.

Between 1980 and 1982, controversy caused by an FBI sting operation that netted members of Congress prompted Attorney General Benjamin Civiletti to issue additional restrictions on covert informants, including oversight over informants who engage in criminal activity.[47]

To increase transparency, Congress amended the Freedom of Information Act, or FOIA, to ensure that the public could obtain government documents and records; these amendments included

34 - 47 See Appendix

added timeframes, sanctions against agencies that wrongfully withheld documents, and fee waivers for journalists.[48] Perhaps most importantly, Congress passed the Foreign Intelligence Surveillance Act, or FISA. FISA created statutory standards for judicially approving electronic intelligence gathering aimed at foreign agents, which were applicable to all U.S. intelligence agencies where the surveillance takes place on U.S. soil.

FISA established a special court made up of seven federal trial judges (later expanded to eleven) appointed by the Chief Justice, and a FISA Appeals Court made up of three trial or appellate justices selected by the Chief Justice to hear appeals. Under FISA, intelligence agencies had to show that the target of electronic surveillance was an "agent of a foreign power." Where the alleged "agent" was a U.S. citizen or lawful resident, there must also exist a connection to federal criminal activity that had been committed or was imminent. The statute explicitly stated that a person could not be deemed an agent of a foreign power solely based on activities protected by the First Amendment.

Additionally, the surveillance had to be for the primary purpose of obtaining foreign intelligence information, and where the surveillance involved a U.S. citizen or lawful resident, the information had to be "necessary" for the conduct of foreign intelligence investigations, as opposed to enforcing criminal law. The FISA court's opinions are classified.[49]

Notably, however, FISA does not apply to all surveillance aimed at foreign intelligence- gathering, but rather places limits on intelligence gathering where it targets U.S. persons or where the intelligence gathering takes place on U.S. soil. At the same time, the Executive Branch maintained plenary authority to carry out foreign intelligence surveillance abroad and against foreign nationals. Successive administrations issued Executive Orders regulating the use of executive authority to conduct intelligence-gathering amid controversy regarding the CIA's role in political assassinations; its use of human experimentation including abusive psychological practices and drugging subjects with LSD; its domestic spying in apparent violation of the National Security Act's prohibition on the CIA having any "internal security" functions; and other egregious abuses of power.[50] These orders culminated in Executive Order 12333 in 1981, which remains in place today subject to numerous amendments.[51]

Executive Order 12333 institutes a number of limits on the conduct of U.S. intelligence agencies, including the CIA. Among other notable restrictions, the Order bans the CIA from engaging in human experimentation or assassinations, influencing domestic public opinion in the United States, or indirectly engaging in any conduct prohibited by the order. The order also requires intelligence agencies to follow applicable federal law, such as FISA and U.S. court orders.

There is some evidence that these reforms in fact did restrain abuses of the COINTELPRO years.[52] However, some of the changes were weak. For example, the lack of direct Congressional authority over the FBI through legislation meant that subsequent Attorneys General could weaken the original guidelines.

Additionally, some evidence indicated that the FBI was not following the guidelines anyway. A Congressional investigation in 1982 found that the FBI's Operation Corkscrew and ABSCAM (FBI codename, a contraction of Arab Scam) sting operations ignored the relevant evidentiary threshold and did not properly vet its informants' credibility pertaining to the guidelines.[53]

In 1983, Attorney General Smith further revised the guidelines by permitting use of speech acts as a basis of investigation and reducing the standards for opening an investigation from "specific and articulable facts" of criminal activity to "reasonable indication" of criminal activity.[54] These changes created enough room for maneuver within the FBI to aggressively surveil and infiltrate the Committee in Solidarity with the People of El Salvador (CISPES), a domestic advocacy coalition that opposed the U.S.-funded right-wing dictatorship in El Salvador. Federal agents monitored meetings, photographed rallies, copied activist paper work, and sent agents to question activists in their homes and elsewhere on the basis of investigating "terrorism" while nonetheless claiming to operate within the guidelines.[55]

The FBI also investigated Palestinian activists on similar grounds, alleging that they were agents of the leftist militant organization Popular Front for the Liberation of Palestine, and collaborated with immigration authorities to initiate deportation proceedings against activists ensnared in the investigation using Cold War- era legislation permitting the deportation of Communists.[56]

Additionally, in the aftermath of the 1993 World Trade Center Bombing, FBI Director Louis Freeh further broadened the interpretation of the existing guidelines, arguing that the "reasonable indication" standard included not only evidence of an imminent violation of the law, but also advocacy of violence with the ability to carry out violent acts.[57]

---

48 - 57 See Appendix

The CISPES spying disclosures prompted Congress to restrict the FBI's domestic spying role with an explicit provision banning the initiation of investigations based on activities protected by the First Amendment. However, this short-lived First Amendment protection was swept aside by the Antiterrorism and Effective Death Penalty Act less than two years later.[58]

At the same time, EO 12333 triggered criticism from the time of its passing over its expansive permission of surveillance despite the limits it placed on intelligence agencies. In particular, critics noted that EO 12333 appeared to directly contradict the language of the National Security Act of 1947 which prohibited the CIA from having any "internal security functions," the Church Committee Report's conclusions about Congressional intent, and multiple federal cases holding that the CIA has no authority to carry out domestic investigations short of investigating potential personnel.

Instead, EO 12333 insinuates that domestic intelligence gathering is permissible where it relates to foreign threats.[59] It further insinuates that regulation of what activities are permissible is limited to internal insight within the Executive Branch.[60]

Abuses of EO 12333 during the "War on Terrorism," discussed below, make clear that these concerns were prescient.

The Antiterrorism and Effective Death Penalty Act and Other Changes

In 1996, in the aftermath of the Oklahoma City Bombing and the first World Trade Center Bombing, Congress passed the Antiterrorism and Effective Death Penalty Act, or AEDPA, which drastically undermined the limited reforms that had been put into place. In creating a new statutory framework, AEDPA discarded the short-lived statutory requirement that barred the FBI from investigating people on the basis of First Amendment-protected activity.

First, AEDPA established a statutory framework that would ban "material support" for any organization designated a "Foreign Terrorist Organization" (FTO) by the Secretary of State. Provided the organization is involved in any sort of armed activity, the Secretary of State has virtually uncontested discretion to label the organization "terrorist."[61]

While the original material support statute prohibited support for certain designated offenses, AEDPA added an additional material support statute criminalizing support to organizations, including forms of support that are unrelated to crime or violence, such as "goods, funds or services."

Second, AEDPA also permitted the government to deport or deny visas to immigrants who were members of designated FTOs or who provided "material support." This was in conjunction with the passage of the Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA) which stripped federal courts of jurisdiction to review otherwise valid deportation orders, even when the orders are pursuant to selective enforcement in violation of the First Amendment.[62] In practice, this meant that even where an immigrant could prove that they were targeted for deportation based on their First Amendment-protected activities, they could not assert the defense in federal court.

By restricting constitutional protections and creating a new "terrorism" statutory framework criminalizing extremely broad categories of conduct, the FBI regained significant authority to target Muslim, Black, and immigrant communities for surveillance and investigation.

At roughly the same time, the Clinton Administration began a program of "rendering" a small number of individuals suspected of "terrorism" offenses to other countries, primarily Egypt. Under this program, individuals convicted in absentia of "terrorism" by the United States government who were captured could be rendered to the United States to face punishment or to other cooperating countries.[63] Some eighty individuals were rendered under this program, and a number of them were reportedly tortured, ordered to be executed after sham trials, or were disappeared by the receiving government.[64]

---

58 - 64 See Appendix

CHAPTER 2

THE "WAR ON TERRORISM" AND THE CONTEMPORARY U.S. SURVEILLANCE STATE

While the history documented above should make clear that the federal government's domestic war on dissent was already well underway before the September 11th attacks, the political crisis the attacks triggered opened the door to significantly greater surveillance and "counter-terrorism" authority by the federal government. These power grabs ultimately shaped the legal and political situation that Muslim, Black, Arab, and immigrant communities currently face.

President George W. Bush declared a "global war on terrorism" within hours of the attacks on the World Trade Center and Pentagon. But rather than using the term as a slogan for a series of new policy directives, the policies adopted by the Bush Administration began to resemble those carried out during an actual armed conflict – even though the attacks were not carried out by state actors and it was unclear whom the war would be against or where it would take place.

Instead, Bush argued that it would be a new kind of war fought on different battlefields that would take place "until every terrorist group of global reach has been found, stopped and defeated."[65] While this new "war" resembled an international campaign of aggressive policing against vaguely defined armed "terrorist" groups, the Bush Administration began asserting the broad legal authority associated with armed conflict to carry out this "war." This included the right to designate individuals as wartime enemy combatants based on their alleged affiliations with "terrorism" and to indefinitely detain, target, and kill them wherever they are and regardless of whether they are taking part in armed combat or not.[66] The "war's" vast scope and its elevation of crime to a matter requiring military responses and reduced judicial involvement resemble the sort of escalations that happened during the "war on crime" discussed in Chapter 1.[67]

With the declaration of this territorially unlimited "war" against individuals and groups that could be designated arbitrarily, as well as those who harbor or support them, the federal government could now use its already broad surveillance authority to criminalize Muslim communities as an extension to prosecuting its new war. Though the government was vague, George Bush made clear nonetheless that the war was aimed at groups that are somehow affiliated with Islam.[68] Mimicking the dichotomy between "dangerous" Muslims who threaten the status quo and "acceptable" Muslims who do not engage in politics, the totalizing and mothering rhetoric of war came to increasingly designate Muslims as the target of a U.S. global war, a reality embodied in various intelligence-gathering efforts the U.S. would pursue.

Above: Seal of the Federal Bureau of Investigation (FBI) outside their headquarters in Washington, D.C. (JL Images)

65 - 67 See Appendix

Fearing Muslims: Preventative Policing & The "Radicalization" Thesis:

In the immediate aftermath of the September 11th attacks, the U.S. government began a mass round-up of immigrants from Muslim-majority countries based on alleged immigration irregularities, held them in detention for months, denigrated them, and deported some to their deaths.[69] Though these mass arrests happened in a moment of crisis, they foreshadowed the enduring suspicion of the U.S. government toward Muslim communities, particularly those of immigrant backgrounds, that underpinned the anti-Muslim ideologies of U.S. foreign policy prior to the attacks and their legitimation afterward.

Soon after, the U.S. government adopted a series of extensive and stringent regulations aimed at Muslim-majority immigrant communities and began engaging in abusive and discriminatory practices within the immigration system to label individual Muslims "terrorist" without providing the opportunity to challenge the accusations. The government implemented the National Security Entry-Exit Registration System, or NSEERS program, which required non- citizen men and boys from twenty-six countries – twenty-five of which were Muslim-majority – to be separately documented, photographed, and fingerprinted, and restricted registrants' places of entry and exit. Failure to comply came with both criminal and immigration penalties.

Similarly, the government criminalized Muslim immigrants as "terrorists" by adding "terrorism"-related accusations in immigration proceedings, which have a lower evidentiary threshold; holding Muslims in detention for minor immigration violations rather than allowing them to be released on bail; carrying out so-called "Third Agency Checks" where intelligence agencies must clear a detained person for removal if they are from a list of Muslim-majority countries; applying extreme interpretations of immigration statutes to Muslims in particular, including so-called "false statement charges"; and filing prejudicial FBI affidavits against Muslims in immigration proceedings.[70]

The targeting of Muslim immigrants immediately after the attacks was premised on a model of viewing Muslims that would extend to all "terrorism"-related policing. Under this model, Muslims are targeted for surveillance before an offense takes place through a number of interlocking mechanisms. Under the preventative policing model articulated by federal officials, "terrorism" can and should be detected prior to a "terrorist" attack, as opposed to the traditional method of law enforcement in which crimes are solved after they take place.[71] The practical effect of this approach is to carry out "anticipatory prosecutions" using expanded "terrorism" statutes and informants who can bait suspects into carrying out actions that meet the decreased standards of "terrorism" violations.[72]

The preventative policing model is premised on the anti-Muslim "radicalization thesis." This thesis, put forward by federal and local officials, posits that signs of Islamic identity can indicate a tendency toward "radicalism" and "terrorist" activity. Similar to previous federal spying programs like RACON that posited, without any basis, that political activity by Muslims signifies "subversive" behavior and by extension threats to the homeland, the Radicalization Thesis makes similar conclusions about Islamic identity. As Amna Akbar notes: "Radicalization suggests that the path from Muslim to "terrorist" is a predictable one produced by or correlated with religious and political cultures of Muslim communities. Government radicalization discourses and programs are almost entirely fixated on Islam and Muslims, despite data that the "terrorist" threat emanating from Muslims is minimal to nonexistent. "[73] FBI documents suggest that "[w]earing traditional Muslim attire," "[g]rowing facial hair," "[f]requent attendance at a mosque or prayer group," "[t]ravel to a Muslim country," "[i]ncreased activity in a pro-Muslim social group or political cause," and "[p]rosletyzing" constitute potential indicators of "radicalization."[74] The entire model is devoid of any empirical validity. In fact, the FBI's own research suggests that "violent extremism is not a linear progression, but an evolving, dynamic situation involving numerous factors, catalysts, inhibitors, and mobilization variables."[75] The assumptions underpinning these preventative models and motives of "terrorism" therefore lack any evidentiary basis.

Nonetheless, the result of this preventative logic puts Muslims in positions of suspicion and vulnerability to prosecution or deportation before an alleged crime has even taken place. A number of statutory changes, federal initiatives, and collaborations across levels of government have facilitated turning this model into policy that expands the scope of surveillance.

Closely related to the preventative policing model and the radicalization thesis is the growth of so-called "Countering Violent Extremism" or CVE initiatives. Sponsored by the Department of Justice, the Department of Homeland Security, and state and local governments, these initiatives provide funding and outreach to Muslim communities to supposedly detect signs of radicalization in youth based on the radicalization thesis discussed above.[76] As these programs are administered by intelligence-gathering agencies and police and are premised on interpreting ordinary behavior among Muslim youth as signals of "terrorism," the programs have provoked significant concern among Muslim communities. Documents obtained by the Brennan

69 - 76 See Appendix

Center through the Freedom of Information Act indicate that at least one CVE program in Minnesota was developed for the purpose of intelligence-gathering and then deceptively marketed to the Somali Muslim community that it was targeting.[77] The programs have been widely condemned by mental health professionals as dangerous, unethical, and potentially illegal.[78]

Invading Muslim Spaces: The Use of Informants, Ethno-Religious Mapping, and Entrapment

From the beginnings of the "War on Terrorism," Attorneys General expanded FBI guidelines to further erode post-COINTELPRO limits discussed in Chapter 1. In 2002, Attorney General Ashcroft expanded the scope of investigations permitted based on speech alone, including permitting agents to visit any place generally open to the public, while expanding which investigative techniques the FBI could use during "preliminary inquiries." Further expansions to the guidelines were made by Attorney General Mukasey in 2008. This set of guidelines would be embodied in the Domestic Intelligence Operations Guide (DIOG), which evidenced the removal of supervisory structures over lower-level agents to engage in investigatory activities of people and groups based on speech. The new guidelines also created another level of investigation, known as "assessments," which did not require any criminal predicate at all. "Assessments" by FBI agents permit physical surveillance and deploying informants. These guidelines were further expanded in 2011.

The breadth of these guidelines are emphasized in a 2010 Department of Justice Inspector General's report discussing the FBI's spying on U.S. activists.[79] The report confirms that the FBI had undercover agents gather information on a number of U.S. advocacy groups ranging from anti-war activists to animal rights groups, including a directive by an FBI supervisor to an agent to spy on leafleting anti-war demonstrators because it was a slow work day. The report, while chastising the decision to send an agent, nonetheless notes that all of the investigative work cited fell within the DIOG guidelines.

The DIOG explicitly authorizes racial and ethnic profiling. The DIOG permits the "collecting and analyzing" of racial and ethnic community demographics, the "geo-mapping" of racial and ethnic demographics, and collecting information about "specific and relevant" racial and ethnic behavior, thereby enabling the types of inaccurate and stereotyped assumptions that conflate religiosity with "terrorism."[80] The use of these tactics appears to plainly violate the Department of Justice's own directives, including its Guidance Regarding the Use of Race by Federal Law Enforcement Agents which prohibits the use of race "to any degree."[81] Records obtained through FOIA requests by the ACLU indicate that the FBI is in fact surveilling mosques and other institutions in Muslim communities as part of an information gathering campaign.[82] Many of these discriminatory tactics were used widely in the immediate aftermath of the September 11th attacks to target people from Muslim-majority countries.

The FBI's guidelines on the use of informants have also been widened. In addition to permitting the planting of informants in communities without indication of criminal activity, the guidelines continue to authorize illegal activity and do not explicitly bar entrapment. While the Radicalization Thesis holds that targets of investigation are predisposed, in reality, agents provocateur often trigger the very radicalization that they are supposedly policing. In the case of Shahawar Siraj, agents consistently attempted to arouse anger in Siraj and repeatedly showed him videos and other materials about violent abuses of Muslims by U.S. and Israeli soldiers.[83] In the case of the Fort Dix Five, agents constantly goaded five Muslim youth into adopting extreme views, mocking their manhood and encouraging them to download similarly inflammatory content that was then used as evidence at trial.[84] Consistently, individuals who display no predisposition are aggressively pushed toward adopting such views, even as they sometimes report the agent to authorities, as in the Fort Dix case. This problem is compounded when targeted individuals are themselves vulnerable due to mental disabilities, financial issues, and the like. The efficacy of such tactics is premised entirely on the questionable assumption that these individuals might have committed the alleged crimes but for the informants' tactics.[85]

Mass surveillance strategies are also used by local police departments that operate under different, mostly non-functional accountability structures. One of the most notorious municipal mass surveillance campaigns against Muslims took place in New York City in 2002, where the NYPD's Intelligence Department created a so-called "Demographics Unit" to systematically map out and spy on immigrants from at least twenty-seven different Muslim-majority countries throughout New York City.[86] The program recruited informants known as "mosque crawlers" from each of those nationalities and systematically logged down religious practices, political speech, and other intimate matters from every mosque within 100 miles of New York City, Muslim student organizations throughout the Eastern seaboard, and Muslim-owned businesses, to track potential indicators of "radicalization." The program did not detect or disrupt a single "terrorist" plot and may have contributed to undermining investigations into at least one plot that was detected through other means. The program was shut down only after its existence was leaked to the press and the

77 - 86 See Appendix

NYPD was required to negotiate multiple lawsuits on the basis that the surveillance program violated a pre-existing settlement agreement from the 1970s in which the NYPD promised not to use such tactics following a lawsuit.[87] Notably, this program was an initiative of the NYPD alone, indicating that the mass surveillance of Muslims is not a purely federal-to-local process.

Brutalizing Muslims: Torture, Disappearances, Renditions, and Secret Detentions

During the "War on Terror," the Bush Administration secretly approved a number of initiatives to torture and abuse detained people, ostensibly in order to extract information from or to degrade them until they were psychologically weakened into divulging information. Though these policies originally were deployed against so-called "High Value Targets" held by U.S. forces and allies, the use of torture as an intelligence-gathering method soon expanded to all U.S. battlefields. Contrary to media narratives of "a few bad apples," torture was sanctioned as a government policy. Specific torture methods were authorized by the highest levels of the government. Torture was used against thousands of innocent people detained either by mistake or for no apparent reason. The refusal to view torture as a crime created interrogation environments in which almost any form of dehumanization, including rape, was considered acceptable. Finally, government officials knew of unauthorized abuse and purposely attempted to shield the abuses from scrutiny by Congress, international monitors, the media, and the rest of the world.

The torture sanctioned by the Bush Administration was authorized at the behest of anti-Muslim neoconservative ideologues who lobbied for legal authorization against veteran military officers who viewed it as a dangerous and discrediting tactic. Torturers often utilized tactics specifically designed to denigrate the Muslim identity of the detained people. Through the use of renditions, secret "black sites," and cooperating regimes, the U.S. and its allies could use or threaten torture against large swaths of Muslim society both in countries that the U.S. occupied with its troops and in countries that were not in a state of armed conflict. The picture of authorization that emerges from all available evidence indicates that the Bush Administration redefined torture as a legal and reliable tactic for intelligence-gathering and redefined potential "terrorist" threats as almost anyone with vague ties to Muslim-majority communities.

Authorizing Torture and Secret Detentions[88]

Six days after the September 11th attacks, George W. Bush signed a Memorandum of Notification bestowing the CIA with extensive discretion to capture and detain individuals suspected of involvement in "terrorist activities" without the oversight of other officials or judicial review.[89] Over the course of the month, the CIA separately began to discuss the idea of finding locations to detain CIA suspects and pressed military leadership to authorize the use of the Guantanamo Bay Naval Base ("GTMO") as a location to operate a detention center as the search for secret detention sites progressed.[90]

In February 2002, Bush signed a directive stating that the Third Geneva Convention, which bans torture and creates protections for prisoners of war, would not apply to the "War on Terrorism" insofar as it was fought against Al Qaeda or the Taliban, the former government of Afghanistan, which began fighting an ongoing guerilla war against the U.S. invasion of Afghanistan. Soon after, Administration officials began looking into the use of the Department of Defense's Joint Personnel Recovery Agency (JPRA), an agency responsible for training U.S. soldiers to withstand torture through a program known as the "Survival Evasion Resistance and Escape" (SERE) training. SERE trainings for U.S. soldiers are designed to degrade and dehumanize captives until they can be forced to say whatever their captor wants. The tactics include forced nudity, extended sleep deprivation, loud music and lights, placing detained individuals in extreme temperatures, violently beating detained people, treating detained individuals as animals, and "waterboarding," a type of torture that simulates drowning. SERE trainings for military personnel are carried out in a controlled environment in which trainees are provided with a safe word. The trainings are not intended to teach trainees how to interrogate, but to resist interrogation.

Nonetheless, by August 2002, Bush Administration lawyer Jay Bybee would write two memos legitimating the use of these torture tactics against those detained by the U.S. government during the "War on Terror." The first memo argued, with no basis, that federal and international law bans on torture only apply to torture that is severe enough that it would cause pain associated with organ failure or death, and that the bans on torture do not apply to psychological torture unless it causes severe and lasting psychological harm. Similarly, Bybee argued without any basis that the bans do not apply to a President acting under defense and necessity. None of these positions have any basis in international or U.S. law. On the same day, Bybee wrote another memo arguing that tactics from the SERE training, including waterboarding, accordingly do not constitute torture. Despite prompting serious concerns from military leaders and lawyers, Administration lawyers tasked with reviewing the proposed tactics consulted only with the few voices suggesting that the tactics were legal and with right-wing policy extremists, such as Douglas Feith and Paul Wolfowitz, who provided no legal basis for the use of these tactics

87 - 90 See Appendix

at all. By December, most SERE tactics, including the use of stress positions, forced nudity, exploiting detained people's fear of dogs, and deprivation of light and auditory stimuli, were approved by Secretary of Defense Donald Rumsfeld. Interrogators began using the tactics at Guantanamo Bay (discussed below).

A little more than a month later, Rumsfeld rescinded his previous approval amid concerns from military leaders. Rumsfeld re-authorized various SERE tactics for use again in April 2003, ignoring the conclusions of a working group and instead favoring memos written by Administration lawyer John Yoo, which repeated Bybee's legal arguments, suggested that Department personnel who use torture cannot be prosecuted, and required specified authorization for additional tactics, which were authorized as a result. In 2004, Jack Goldsmith, another Administration lawyer, rescinded the Bybee memoranda.

But by then, it was too late. The legal memoranda legitimating torture and the ambiguity about which types of torture tactics were approved created an environment where avoiding torture was seen not as a legal obligation but a policy preference. Notably, even during times when the approvals for such tactics were rescinded, military leaders in Iraq and JPRA staff either ignored the rescissions or did not even receive them. As a result, even when the torture methods were rescinded briefly in 2003 and in 2004, U.S. military leaders and the CIA continued using them. And while the Bush Administration's declaration regarding the application of the Geneva Conventions did not apply to Iraq, standard operating procedures and rules developed during this period legitimated the use of SERE tactics across both Afghanistan and Iraq.

U.S. Torture of Detained People at GTMO and CIA Black Sites

Holding hundreds of detained people from foreign battlefields at GTMO, the CIA began interrogating a number of so-called "high value targets" prior to the authorization of torture tactics. The U.S. government's position that the Third Geneva Convention does not apply to individuals detained in their war against Al Qaeda or the Taliban and that their detentions would not be subject to the review of federal courts would be at issue in a series of court battles spanning from the initial use of the base as a detention facility to the end of the Bush Administration.[91] During this time, however, the U.S. government's interrogations of some detained individuals utilized torture. At the same time, the CIA began operating a network of secret "black sites" to detain and torture people across the world; these sites were organized in secret and were hidden from the public until they were leaked to the press.[92] People imprisoned in black sites were subsequently transferred to GTMO after the revelations.[93]

In total, the CIA detained at least one hundred and nineteen people through its secret detention program, though the actual number may be considerably higher as the CIA did not maintain accurate records; by the final year of the program, the CIA was involved in the detention of some three thousand people alongside other intelligence agencies.[94] Of the at least one hundred and nineteen individuals known to have been detained by the CIA, at least twenty-six were held despite apparently not fitting under the Memorandum of Notification, and a number of detained people who were brutally tortured were later determined to be captured due to mistaken identity.[95]

At least thirty-nine of the detained people were tortured.[96] At least five detained people were subject to "rectal feeding," and one was apparently anally raped. Some detained people were told that their family members and children would be tortured. Detained individuals with broken legs and feet were forced to stand on their injuries. Detained people were threatened with death by guns and electric drills and were made to believe others had been executed in front of them.

Detained individuals were subject to extensive waterboarding, prompting violent convulsions and vomiting, nearly drowning some individuals. Some detained people were subject to extreme temperatures and endless loud music. Detained people were sometimes deprived of sleep for up to one hundred and eighty hours. At least one detained individual was killed under torture when he was left chained to a wall in cold temperatures. Many of the tactics utilized were not authorized; nonetheless, no one from the CIA was ever disciplined or subject to criminal charges. The CIA repeatedly lied to Congress, the media, and others about the sheer brutality of tactics utilized by interrogators and overstated their value in obtaining information. In reality, any useful intelligence was obtained without torture and detained people were tortured regardless of whether or not they complied.

Expanding Extraordinary Renditions

Apart from the use of torture and detentions by the CIA, the Bush Administration expanded the relatively small extraordinary renditions program that existed under the Clinton Administration, permitting the CIA to render detained people to third countries known to engage in torture for the sole purpose of interrogation even when they had not been charged or convicted of any "terrorism" offense.[97] The CIA was suddenly authorized to nab individuals without any oversight to be sent to third countries, including Egypt and Syria, where they were electrocuted, kept in grave-like cells, and otherwise abused. A number of the individuals kidnapped by the CIA and rendered were people

91 - 97 See Appendix

with no apparent links to "terrorism," and some were taken by mistake.[98] It is unclear exactly how many people were rendered, though the U.S. carried out at least one hundred extraordinary renditions between 2001 and 2005.[99] All victims of this policy were Muslim. In one particularly grisly example, Maher Arar, a Canadian Muslim of Syrian descent was rendered to Syria and brutally tortured when he was stopped by U.S. officials on a layover in New York on his way home to Canada from a vacation in Tunisia.[100] After answering affirmatively that he knew another individual from his early childhood that, unbeknownst to him, was an Al Qaeda suspect, Mr. Arar was detained and rendered to Syria, where he was ruthlessly beaten with shredded cables and held in a small cell for nearly a year before being returned to Canada.[101]

U.S. Torture in Iraq and Afghanistan Invasions

Rumsfeld's multiple and conflicting suggestions about which torture tactics were acceptable and under what circumstances, alongside the Administration's decision not to view the ban on torture as a legal obligation, ensured that U.S. torture tactics would not be limited to "high value detainees" held at Guantanamo Bay or the CIA's other black sites (where torture tactics were still nonetheless illegal). Soon after the December Rumsfeld memoranda approving various SERE tactics, Standard Operating Procedure (SOP) manuals for U.S. soldiers in Afghanistan greenlighted these tactics.[102] Shortly after the authorization of the use of these tactics by Rumsfeld but before the leaks about the U.S. military's use of torture, some eighty-eight people were tortured by the U.S. military and CIA in Afghanistan, mostly from 2003 to 2004.[103]

But it was in Iraq that the barbarism of the U.S. torture policies triggered international outrage and backlash. Though Iraq was not covered by the Bush Administration's decree to ignore the Third Geneva Convention and the war in Iraq was not against Al Qaeda or the Taliban, SERE tactics began showing up in the SOPs for U.S. forces in Iraq soon after they appeared in Afghanistan. By the summer of 2003, these tactics were found in virtually all SOPs for all military units in Iraq.[104] In September of that year, the JPRA sent a team to Iraq to assist in interrogations as U.S. forces in Iraq became increasingly desperate to break detained individuals. The advent of SERE tactics and the generalized desire to break down detained people created a climate in U.S. military detention facilities in Iraq that "condone[d] depravity and degradation rather than humane treatment of detainees."[105] At the same time that U.S. forces in Iraq became increasingly hostile toward those they detained, the aggressiveness with which U.S. occupation forces sought to capture insurgents and pacify Iraqi society escalated the number of raids carried out and the breadth of whom these raids captured. U.S. soldiers began carrying out mass arrests, including of women and children, detaining and arresting reporters, among others.[106] Estimates indicate that some ninety percent of Iraqis detained in U.S. military dungeons in Iraq were detained by "mistake."[107] Military interrogators were encouraged to "soften up" prisoners for interrogation to obtain the intelligence necessary to stop insurgent attacks.[108]

The degrading and dehumanizing conditions which the U.S. imposed upon its Iraqi subjects in Iraq would be captured on camera and released to the world in 2004.[109] That year, photos leaked to the press showed U.S. personnel violently and sexually abusing detained people at the Abu Ghraib prison, which housed a combination of individuals accused of committing crimes against Iraqis as well as suspected insurgents. The photos portrayed, among other things, detained people being forced to engage in sex acts with themselves and with each other while their captors smiled at the camera. Investigations carried out prior to the leak documented the punching and kicking of detained people; forcing detained individuals into sexually explicit positions; forcing detained people to masturbate; forcing male detained individuals to wear women's underwear; forcing male and female detained people to pose nude; arranging nude detained people into a pile and jumping on them; simulating the electrocution of nude detained people; raping a detained woman while forcing another detained individual to watch; sodomizing a male detained individual with objects; pouring phosphoric liquid onto detained people; threatening detained individuals with rape; accosting detained people with dogs; smearing feces onto detained individuals; and forcing detained people to eat feces. Other individuals were violently beaten to death and had their dead bodies photographed. Journalists have separately alleged that women who were raped at Abu Ghraib became pregnant and were killed by their families out of shame.[110] Seymour Hersh, one of the investigative reporters who revealed the story, indicated that there are likely tapes from Abu Ghraib that depict U.S. soldiers sodomizing children.[111] It was also noted that the photographs themselves were apparently a form of torture by frightening detained individuals with the possibility that sexually compromising photographs of them could be circulated after their release.

U.S. officials were apparently aware of the conditions at Abu Ghraib, which were repeatedly reported by the Red Cross; in response, the government threatened to restrict access to the Red Cross. Some of the lower-level prison officials were charged with criminal offenses.[112] Nonetheless, reports of abuse and torture by U.S. forces in Iraq continued after the Abu Ghraib scandal.[113]

---

98 - 113 See Appendix

President Obama's Weak Reforms

The Bush Administration repeatedly reaffirmed the legality of SERE torture tactics, even upon the revelations of abuse by the CIA and the Abu Ghraib prison scandal.[114] It was not until the presidency of Barack Obama that some high-level policy changes were made.

First, Obama issued multiple executive orders regarding torture, interrogations, and detention. One order officially ended the CIA's use of secret detentions and required all U.S. interrogations by any agency to follow the Geneva Conventions as a baseline and use only the U.S. Army Field Manual, which recognizes the Geneva Conventions, for guidance.[115] Another order set up a task force to review detention policy more generally.[116] Soon after, the Obama Administration issued new guidelines for the transfer of detained individuals to other countries, requiring Inspector Generals of other Administration departments to oversee each case and obtain assurances from third countries that rendered individuals would not be tortured.[117]

The Obama Administration's changes, however, left considerable shortcomings. First, the Army Field Manual arguably still permits certain types of interrogation techniques that qualify as torture, including sleep deprivation and separation, despite not including SERE tactics.[118] Second, critics noted that the changes to the rendition program were classified, making it difficult to evaluate if the U.S. government was still engaging in extraordinary renditions. The changes lent significant credence to the assurances of third countries and furthermore, nothing under the Obama Administration's changes barred the government from simply requesting that foreign intelligence agencies carry out the arrest themselves.[119] Finally, the Obama Administration refused to prosecute anyone involved in the approval of torture and continued to invoke Executive privileges to prevent civil litigation against the CIA and others complicit in torture.[120] This is significant as it failed to reaffirm the recognition that torture is a crime warranting legal sanction rather than a policy preference, which was fundamental to the widespread use of both approved and unapproved torture tactics under the Bush Administration.

Note that although Obama's policy changes did reduce the use of torture, they did not alter the authority claimed by the U.S. government to indefinitely detain individuals whom the U.S. alleged to be members of Al Qaeda, and in fact this authority was expanded during the Obama Administration. In 2012, the U.S. Congress passed an amendment to the Authorization for the Use of Military Force (AUMF)—originally passed to target those involved in the September 11th attacks—that expanded the authority to carry out such detentions to anyone associated with Al Qaeda without a geographic scope. As such, while the availability of legal redress has been expanded since the Bush Administration began its project of detentions, the process remains one providing the Executive Branch with extreme authority to continue detaining individuals. Nearly twenty years after the opening of GTMO, the U.S. government continues to detain at least forty- one people there, aside from individuals detained in other places.

Torture and Surveilling Muslims

The use of torture is the most glaring example of a pattern that is consistent through all of the aggressive intelligence-exacting measures that have been aimed at predominantly Muslim communities under the guise of carrying out a "war." The widespread use of torture not only indicated that the government was willing to disregard all normally binding laws, but did so for the sake of using tactics that the government knew to be useless for obtaining information from most of the individuals it subjected to torture. U.S. officials knew or had reason to know that a significant number of the individuals they tortured did not even have useful information. Nonetheless, the U.S. government carried out an expansive, illegal, and secret campaign of detaining and torturing individuals whose only identifiable commonality was that they were from Muslim communities. Like other overboard and abusive methods to obtain information, much of it useless, the government's campaign of torture emphasized how surveillance tactics are a means of control and subordination rather than an effort to obtain important information.

Criminalizing Muslim Society: Prosecutions for "Material Support":

The 2001 USA PATRIOT Act expanded the definition of the already vague term "material support" to designated "foreign terrorist organizations" (FTOs) that could be criminalized by adding "expert advice or assistance" to the list of prohibited forms of support. The preventative policing model's application to Muslims has been on full display through the abuse of the already expansive "material support for terrorism" statutory framework that was passed through AEDPA.

The material support statute is broken down into multiple parts. The first, 2339A, criminalizes support for various offenses which are characterized by the statute as "crimes of terrorism." The second, 2339B, criminalizes support for groups that the United States government has designated as "foreign terrorist organizations." The expansiveness of both statutes permits prosecutions of individuals over apparently benign activity.

Prosecutions under 2339A are particularly open-ended where they are used to prosecute so- called "unaffiliated"

114 - 119 See Appendix

"Like other overboard and abusive methods to obtain information, much of it useless, the government's campaign of torture emphasized how surveillance tactics are a means of control and subordination rather than an effort to obtain important information."

individuals accused of "terrorist" activity. The underlying offenses which 2339A prohibits include a variety of federal crimes. Likewise, because 2339A is not tied to the FTO list, there is no requirement that the person accused of providing material support actually be involved in any designated "terrorist" organization. The statutes listed for violation by 2339A themselves include so-called "inchoate offenses" in which someone has not actually carried out the underlying violation but has attempted or agreed to do so: both material support statutes include conspiracy and attempt liability. The effect of the breadth of the statute is that an individual can be prosecuted when accused of conspiring or attempting to provide the kinds of "support" toward violations of the statute. Where "conspiracies" can be defined broadly – including "the global jihad" movement, for example[121] – an individual can be prosecuted for material support violations where, despite having no actual connections with those associated with "terrorism," their independent activities somehow assist in the commission of crimes by others, even if those crimes have not yet taken place.[122] As a result, a person could be tried for conspiracy to provide material support toward a conspiracy to violate the law. In short, the statutory framework permits extremely broad prosecutions. Examples include prosecuting an individual for online speech that prosecutors allege to be a form of recruiting for the abstract international jihadist conspiracy, which is not an actual organization,[123] or an attorney passing messages to a person accused of "terrorism" that could have hypothetically enabled them to further "terrorism"-related organizing.[124] Actually accomplishing any of these tasks is unnecessary to find liability.[125]

2339B prosecutions also criminalize material support in an overbroad fashion, where otherwise benign interactions between targets of prosecution and designated organizations can be criminalized. One egregious example of such a prosecution was of the Holy Land Foundation.[126] The Holy Land Foundation, once the largest Muslim charity in the United States, was accused of providing humanitarian aid supplies to zakat (charity) councils in the Israeli-occupied Palestinian Territories. Though the U.S. government provided aid through the same councils and continued to do so after the Holy Land Foundation prosecution, the government argued that aid to the councils constituted material support for "terrorism." Specifically, the prosecution argued that the councils had a close relationship to Hamas, a Palestinian organization designated as an FTO by the United States government which had, during the intervening time, taken control over the zakat councils as a result of its 2006 election victory. Based on this reasoning, legitimate humanitarian aid to the councils that was not materially different from the kind of aid provided to the same councils at the same time by the federal government was found to violate the material support laws when carried out by the Holy Land Foundation.

Alongside using secret Israeli military witnesses at court, hampering defense counsel's ability to cross examine, the prosecution sought to tie the defendants to Hamas through political speeches that the defendants had given. That the U.S. government had not designated the zakat councils themselves as fronts for Hamas, had not restricted financing of them, and had not avoided sending funds to these councils through the U.S. AID Program itself, was irrelevant to the Holy Land Foundation prosecutions and ultimate convictions.[127]

This expansive statutory scheme allows prosecutors to target every day and otherwise protected activity in Muslim communities, from political advocacy to charity, on the grounds that the advocacy could somehow be linked to vaguely defined concepts of "terrorism." This statutory authority, already prone to abuse, makes the large amounts of information collected by federal agencies through expanded surveillance authority much more dangerous to Muslim communities.

Programmatic Mass Surveillance

Both the declaration of a "war" against "terrorism" and the U.S. government's military invasions of multiple countries, particularly Iraq, came with aggressive expansions of its use of bulk data surveillance. Much of this surveillance was coordinated by various agencies through the use of the National Security Agency, which views other branches as its "customers," and the FBI. Soon after, the system of surveillance constructed by the NSA would become effectively unlimited in its mass collection of virtually all accessible electronic data with no meaningful geographic or legal limitations for large numbers of people.

Authorizing Mass Surveillance: Statutes and Directives

Shortly after the September 11th attacks, the Bush Administration began the "Presidential Surveillance Program" (PSP) in secret based on the authority of EO 12333 (discussed above) and outside the bounds of the Congressional FISA statute altogether.[128] Though EO 12333 is aimed at foreign intelligence gathering, the program empowered the NSA to carry out domestic wiretapping, e-mail interception, and call metadata[129] gathering without warrants when they claimed that the individuals targeted within the United States were linked to persons connected with "terrorism" abroad.[130] According to legal memos from the White House Office of Legal Counsel, White House lawyers like John Yoo argued that this program was not governed by FISA and that even if it was, the President nonetheless had the unilateral authority to carry out domestic spying for national security purposes.[131]

---

121 - 131 See Appendix

As part of the program, the Executive Branch authorized itself to collect vast amounts of data with the compelled collaboration of major U.S. telecommunications companies.[132]

At the same time, Congress passed the USA PATRIOT Act which made a number of significant changes and created considerable expansions to the government's already broad and expansive surveillance authority. First, Section 215 of the USA PATRIOT Act expanded the authority of the FBI to subpoena business records as part of foreign intelligence investigations. The post-9/11 rules removed any requirement that the target of such subpoenas be suspected of being an agent of a foreign power, and the items that could be subpoenaed were expanded to "any tangible thing." As long as the records sought were "relevant" to an authorized investigation under FISA, the government could obtain records.[133] The FISA Court would later accept a broad definition of "relevance" under Section 215 that would extend to all telephone metadata from all major U.S. telecommunications carriers. The FISA Court justified this interpretation on the basis that collecting irrelevant data was necessary to identify relevant data.[134]

The USA PATRIOT Act which stands for "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism" also expanded the government's authority to issue "National Security Letters" (NSLs) requesting certain business records without a FISA court order at all. National Security Letter authority had previously been given to allow the FBI to obtain certain types of financial and consumer activity records where the records pertained to a national security investigation despite various federal statutes that otherwise limited government access to such records. These statutes generally contained provisions allowing the FBI to prevent disclosure of, or "gag," the request for the records. The USA PATRIOT Act expanded the authority of the FBI to obtain records by enabling lower-level FBI officials to issue NSLs, eliminated the requirement that NSLs must pertain to a foreign agent or power and simply be "relevant" to an investigation, and created new grounds for issuing NSLs that permitted any intelligence agency involved in "terrorism" investigations – not just the FBI – to issue an NSL. In 2003, the Attorney General issued guidelines permitting the request for NSLs during "preliminary investigations," prompting a spike in issuances.[135] The 2006 re-authorization of the USA PATRIOT Act added specific penalties for violating the non-disclosure of requests for records and provided for judicial enforcement of the NSLs.[136]

The FISA Court's scope itself was also drastically expanded after the September 11th attacks. The USA PATRIOT Act culled the original limits of the FISA Court's separation between traditional domestic criminal law enforcement and foreign intelligence gathering. Rather than requiring that investigations under FISA be limited to those in which the "primary" purpose of the investigation was gathering intelligence information, the post-9/11 FISA only required that foreign intelligence gathering be a "significant" purpose. This effectively eliminated the traditional "wall" between foreign intelligence gathering and criminal investigations. As a result, the FBI and other agencies seeking to prosecute criminal offenses taking place entirely within the United States, including material support for "terrorism," could use the FISA Court's lenient procedures rather than the strict rules of Title III and by extension, the Fourth Amendment.

It is worth emphasizing that even where newfound surveillance authorities remain tied to investigating particular individuals as potential foreign agents, including as "terrorists," the authority is overbroad. Like in the CISPES investigations of decades prior, legal limits on what evidence indicates that someone may be a foreign agent contradict any meaningful exclusion of First Amendment activities such as religious and political activity.[137]

It was not until 2013, however, when former NSA contractor Edward Snowden leaked classified documents to journalists that the scale of domestic and international spying carried out by the U.S. government was revealed.

Mass Surveillance in Practice

The sheer scope and expansiveness of the government's newfound surveillance authority is difficult to convey properly without a brief discussion of the NSA's involvement in the U.S. government's military campaigns overseas, particularly in Iraq. In the lead-up to the war, the NSA spied on United Nations delegations as part of the aggressive diplomatic push to pressure other nations to support the questionable legitimacy of the U.S. invasion of Iraq.[138] Once the U.S. military invasion and occupation of Iraq was underway, the NSA embedded its agents among U.S. troops to gather intelligence and to coordinate its global spying with the military, telegraphing the NSA's expansion and the honing of its intelligence-gathering practices.[139]

During the occupation, the NSA set up campaigns to gather virtually all Iraqi telecommunications data, including the private networks of the Al Jazeera media station in Iraq and multiple Iraqi government ministries.[140] At the same time, the NSA coordinated with U.S. interrogators in Iraq as well as with the CIA's efforts to render and torture detained people at the U.S. military facility at GTMO, discussed above.[141] In Iraq, NSA technicians sorted through computer files seized during raids to find pornography in order to shame and sexually humiliate religious Muslim

132 - 141 See Appendix

detained individuals, force detained people to watch it as punishment, or offer the pornography as a reward to detained people in exchange for compliance.[142]

The use of mass intelligence-gathering in Iraq presents a microcosm of the type of information that the U.S. government sought for its new "war" everywhere. Far from limiting its surveillance to countries that it had invaded, the U.S. government utilized the authorities of EO 12333 to engage in mass surveillance on a global scale, coordinated primarily through the NSA. In its efforts to engage in "foreign intelligence" gathering, the NSA:

- spied on international medical nonprofits;[143]
- tapped into Yahoo and Google internal servers from hundreds of millions of customers including, address books and contact lists;[144]
- gathered hundreds of millions of text messages and mined contacts, location data, and credit card details;[145]
- gathered webcam images, including intimate ones, from Yahoo and possibly other companies;[146]
- bypassed civilian leaders in other countries to establish intelligence-sharing relationships with their militaries;[147]
- set up a sprawling surveillance network for the Ethiopian government in spite of its numerous human rights abuses;[148]
- intercepted mobile phone and satellite data throughout Lebanon, Palestine, and various Arab countries during the Arab uprisings of 2011 in coordination with the British government;[149]
- intercepted GSM phone data for the purpose of locating targets to carry out drone strikes in Afghanistan and Iraq;[150]
- intercepted communications at internet cafes across Iraq, Iran, Yemen, Syria, and Lebanon;[151]
- spied on European anti-war activists and subsequently demanded their arrest (based on accusations of links to "terrorism" that Italian courts rejected);[152]
- shared raw intelligence, including information pertaining to U.S. citizens, with Israel;[153]
- transferred mass spying programs from the Iraq and Afghanistan wars to the U.S.-Mexico border;[154]
- spied on private communications of diplomats and political leaders throughout the world, including monitoring the cell phone of German Chancellor Angela Merkel;[155]
- recorded the contents of every domestic and international phone call in several countries, including the Bahamas and Afghanistan;[156]
- collected information from cell phone apps, including ads linked to the game "Angry Birds";[157]
- and engaged in countless other repressive and abusive spying practices.[158]

---

142 - 158 See Appendix

"The NSA built a massive searchable database called XKEYSCORE containing emails, Facebook chats, browser history, and even username and password combinations." [159]

Notably, the programs in question, even when aimed at individuals outside of the United States, were virtually guaranteed to collect the information of U.S. persons because of their sheer scope and the international nature of most of the data these programs were gathering.[160] Just as U.S. spying in the Philippines a century earlier ensured that the surveillance state would not be limited to "foreign" targets, the NSA's mass surveillance efforts targeted U.S. citizens and residents, including their electronic communications and communication records.

By 2004, the NSA had set up experimental blimps to capture wireless signals in Maryland[161] and gathered signals intelligence to monitor the 2004 Republican and Democratic National Conventions and the Olympic Games in Salt Lake City.[162] This is unsurprising: the U.S. government had authorized itself to gather information domestically without going through the FISA process based on the highly dubious memoranda discussed above.

Using the NSL authority, the FBI began aggressively obtaining internet and financial data regarding thousands of subscribers and customers from financial and internet institutions, alleging that such records were relevant to "terrorism" investigations. The Department of Justice's Inspector General released a report in 2007 indicating that the FBI repeatedly violated the authorizing statutes to obtain NSLs, did not implement proper supervisory controls, and contained inaccurate information about whether the target was a U.S. person.[163] The report indicated that the 143,074 NSLs that the FBI issued between 2003 and 2005 were themselves a significant undercounting where the FBI failed to properly track these letters.

By 2005, a majority of the individuals targeted with NSLs were U.S. persons. Moreover, each letter sometimes included multiple requests. The next year, following the use of NSLs under the re-authorization of the USA PATRIOT Act, the Inspector General noted a continued trend of using NSLs against U.S. persons and the failure of the FBI to sufficiently justify gag orders.[164]

Separately, without any apparent statutory justifications, the FBI issued so-called "exigent letters" to obtain telephone records. These were effectively informal requests for personal records justified on the premise of an impending emergency. The Inspector General's reports noted that such requests violate the Electronic Communications Privacy Act, one of several statutes authorizing NSLs.[165] Instead, the FBI regularly issued such requests without keeping track of them and apparently fabricated claims of "emergency" in order to avoid the legal process of obtaining the records sought.

Furthermore, the FBI contracted with three telecommunications companies to have FBI personnel located at their companies in order to carry out exigent requests without any legal process, and even to carry out so-called "sneak peek" searches in which the stationed agent would simply obtain the information over the shoulder of the telecommunications employee. The FBI apparently lied to the FISA Court multiple times when using information obtained through exigent letters to justify requests for a wiretap, spied on reporters using exigent letters to investigate a leak, and tried to retroactively justify the exigent letters with "blanket" NSLs.[166]

Leaks and Statutory Authorizations

Amid an original controversy following leaks of some aspects of the Presidential Surveillance Program (PSP) in 2005 by journalists, long preceding the more revelatory Snowden leaks, the Bush Administration began utilizing the existing FISA framework to carry out some of the domestic spying originally carried out under the PSP. Specifically, the gathering of phone metadata through the so-called "Call Detail Records program" was refashioned to operate under Section 215 of the USA PATRIOT Act and subject to limited FISA Court oversight.

Additionally, Congress passed the FISA Amendments Act (FAA) at the behest of the President, who moved the so-called "Terrorist Surveillance Program" (TSP) under the FISA framework. The TSP authorized intercepting communications held by domestic U.S. carriers in which one communicant is a non-U.S. person located overseas. These expansive programs are discussed below.

159 - 166 See Appendix

These expansive programs are discussed below.

While the changes were carried out under the auspices of respecting the oversight of the FISA process, the details show that in fact, the FISA Court became a rubber stamp in the mass surveillance programs of the Executive Branch.

The Call Detail Records Program

Under the Call Detail Records (CDR) program initiated by President Bush under the PSP from 2001 to 2006 and subsequently authorized under Section 215, the NSA, operating with the signature of the FBI, gathered hundreds of billions of telephony metadata records each year of subscribers to all major U.S. telecommunications companies. Every ninety days, telecom companies were required to turn over all subscriber metadata based on an order from the FISA Court which apparently rubber stamped these requests for mass surveillance.[167]

The data obtained by the NSA indicates which particular phone number dialed which number, when each call was made, and how long each call lasted, but does not include the contents of any calls. NSA officials have emphasized the lack of content recording to defend the program's consistency with privacy. But metadata is itself incredibly revealing, not only exposing intimate relationships and patterns among callers (for example, proving that a particular person has made a call to a suicide hotline or an abortion clinic, or repeated calls to an ex-spouse), but also outlining the web of personal contacts each collected number has dialed.[168] Indeed, even a covert CIA operation to illegally kidnap a suspect in Italy under the extraordinary renditions program (discussed below) was uncovered by Italian investigators through the CIA agents' cell phone metadata.[169] As a government oversight board indicated, the CDR program, even when operating under the auspices of the secret FISA court, appears to violate multiple laws.[170] Aside from the strained definition of "relevance" accepted by the Court which determined that all U.S. subscribers' call information could be viewed as "relevant" to an investigation, Section 215 itself only authorizes the FBI – not the NSA – to obtain information, does not permit information that has no apparent link to an investigation at the time it is collected, and only applies to existing records rather than to records that had not been collected at the time. When searching the database of call records, NSA officials were in charge of determining whether a search fit the statutory criteria, and repeatedly queried records of U.S. persons that they should not have and carried out at least one automatic search of numbers that were not approved for search. While the NSA did report these "errors," the fact remains that the NSA was in control of large quantities of domestic telephone records in apparent violation of the language of the statute and without any oversight as to how they were searched. Due to the lack of particularity, the government was entrusted to enforce the reasonableness inquiry rather than a neutral judge.

Above: The ominous Room 641A at an AT&T facility in San Francisco is allegedly one of the rooms in which the NSA gathered virtually all data communications from AT&T subscribers (M. Klein).

The "Terrorist Surveillance Program" and FISA Section 702

While the government created a database containing millions of call records through the CDR program, following the 2005 leaks it also sought to bring its mass surveillance of communications held domestically under the FISA framework through the FAA. However, under Section 702, no individualized warrant would be required by the FISA Court for communications in which at least one communicant is a non-U.S. person reasonably believed to be overseas, communications obtained for any foreign intelligence purpose, or communications about a selector tied to such a person.[171] Such communications can be intercepted, as well as communications about the target, under a single, periodically expiring FISA Court order against the carrier. Instead of an individualized warrant, the government would issue a 702 order to telecommunications companies to periodically collect large quantities of subscriber information and data from private internet companies, such as Google, Facebook, and Microsoft (the "PRISM" program), as well as "backbone" internet providers whose equipment makes up the telecommunications infrastructure of the Internet, like AT&T and Verizon (what the NSA called "Upstream" surveillance). Although U.S. persons are not to be targeted, any communications between a U.S. person and someone fitting the broad targeting description can be collected "incidentally," as could any communication about the specified selector. Because the targets were not limited to suspected "terrorists" but simply anyone who may have relevant "foreign intelligence information," the NSA could target communications between and about hundreds of thousands of individuals.[172] To carry out Upstream collection, the NSA would tap into network cables at major internet service providers at various hubs, such as eight different AT&T buildings, in order to gain access to large quantities of internet traffic.[173]

167- 173 See Appendix

Through these programs, the NSA collected hundreds of millions of electronic communications, including e-mails, text messages, photos, and online chats, many of them involving U.S. persons.[174] For some time, the NSA also collected so-called "multiple communications transactions" or MCTs, which are data that, for technical reasons, could not be collected without collecting both the target communication and other discrete communications. This data would then be shared, subject to some "minimization" procedures regarding data involving U.S. persons, with other intelligence agencies.

"...suspicious activity reporting involves the collection of significant amounts of apparently innocuous information."

The 702 surveillance program is assailable on numerous grounds. First, although the program was an attempt to ensure compliance with FISA, it essentially operates without any FISA Court oversight at all. Indeed, in a 2011 FISA Court opinion that was declassified after the Snowden leaks, the FISA Court indicated its frustration with being repeatedly misled about the scope and type of communications that the NSA was gathering on multiple occasions, specifically when the NSA collected MCTs without authorization and when the NSA had misrepresented the phone metadata it was gathering.[175] Only after NSA agents themselves disclosed the error in representing what data was gathered could the FISA Court issue an opinion calling the program into question, which ultimately prompted the NSA to purge some of the Upstream data it collected. Second, the statute, even when followed strictly, permits obtaining the information of hundreds of thousands of communications in bulk with the awareness that many communications are not permitted by the statute as they include "about" communications among "U.S. persons." Furthermore, if U.S. persons are surveilled consistent with the statute, it is only because the statute permits mass surveillance: no one is targeted. Third, the mere collection of large quantities of data that could – and were – searched by NSA agents, including a sizeable amount of U.S. person data searched by mistake, without the requisite court oversight to ensure that NSA agents were not abusing the system, meant it was ripe for abuse.[176] Indeed, NSA agents on several occasions are known to have used the agency's spying authority to spy on love interests.[177]

Federal and Local Surveillance Collaboration

While federal and municipal agencies have different and often competing programs, the post- 9/11 climate also created a series of federal, state, and local police collaborations, such as the sudden creation of dozens of new FBI Joint Terrorism Task Forces at FBI offices throughout the country, intelligence-sharing initiatives, such as the FBI's eGuardian, and the Department of Homeland Security's competing Information Sharing Environment (ISE) and its network of "fusion centers."

Closely associated with the preventative policing model, these information-sharing initiatives include the use of "suspicious activity reporting," an additional form of mass surveillance in which civilians and law enforcement alike are encouraged to report activities, untethered from criminal conduct, that could supposedly thwart a terror attack. But because there is no criminal predicate required, suspicious activity reporting involves the collection of significant amounts of apparently innocuous information. Suspicious activity reports are gathered and shared through fusion centers and among intelligence agencies.[178]

Through these initiatives, large amounts of information are shared subject to conflicting guidelines across local, state, and federal agencies, and are retained for long periods of time.

While the guidelines for what kind of information is gathered through these competing and collaborating initiatives vary, they do not require a nexus to criminal activity. Rather, the premise of these initiatives is that collecting large amounts of information will permit intelligence agencies and the police to detect the existence of a plot based on disparate pieces of information.[179]

Nonetheless, a scathing Congressional investigation on fusion centers concluded that "reporting from fusion centers was often flawed, unrelated to terrorism…outdated, duplicative and uninformative"; that reporting officials "repeatedly violated guidelines" but "faced no sanction"; that fusion center detailers were not "sufficiently train[ed]…to legally and effectively collect and report

174 - 179 See Appendix

intelligence"; that the retention of data violated the Privacy Act; that "fusion centers have been unable to meaningfully contribute to federal counterterrorism efforts"; and that "fusion centers may have hindered, not aided, federal counterterrorism efforts."[180]

Some Reforms

The government faced considerable public scrutiny when Edward Snowden, an NSA contractor, revealed the sheer scale of the NSA's surveillance. As such, some limited reforms were implemented. First, Congress passed the USA Freedom Act.[181] This Act placed certain transparency measures and restrictions on the use of National Security Letters, explicitly limiting them to only an individual subscriber and adding judicial review mechanisms where a recipient wants to challenge the associated gag order. Congress allowed Section 215 of the USA PATRIOT Act to sunset in 2015, and through the USA Freedom Act, replaced it with a modified version of the CDR program that would require telecommunications companies to store metadata being requested by the NSA, and would require the NSA to request specific data when making applications to the FISA Court, along with other limited oversight mechanisms.[182] The program was ultimately discarded by the NSA in 2018 (discussion below).

Unfortunately, the USA Freedom Act expanded the authority under Section 702 as efforts to end the collection of U.S. person data and other reforms were shut down. Instead, the USA Freedom Act expanded the definition of an agent of a foreign power. On its own, the NSA ended its use of Upstream collection of "about" communications in 2017.[183]

Lastly, to address the enormous bulk surveillance of information about non-U.S. persons by U.S. intelligence agencies, the President passed Presidential Policy Directive 28 (PPD 28), which issued nominal restrictions on the gathering of foreign intelligence. However, commentators have noted that many of the requirements were already present, and that in fact, no additional, meaningful restrictions were placed on foreign intelligence gathering.[184] The Privacy and Civil Liberties Oversight Board had originally sought to audit spying taking place under EO 12333; before the report was published, however, PCLOB was essentially dismantled.[185]

Watching Muslims

The massive electronic surveillance expansions in the aftermath of 9/11 gathered immense amounts of data from millions of people, and the international targets of the dragnet varied. But the primary targets for domestic surveillance were Muslims and individuals deemed in some way connected to the Islamic diaspora. Because of the vagueness of those authorities, the secrecy with which the NSA conducted its espionage, and the unbound nature of these programs, it should not be surprising that the FBI and NSA systematically spied on Muslims, including prominent Muslim citizens of the United States.

For example, even though Section 702 explicitly bars spying on U.S. persons, leaks indicated that among the thousands of mostly Muslim non-U.S. persons whose e-mails were intercepted by the NSA, the NSA monitored the e-mails of several prominent U.S. citizens and residents who were active in domestic U.S. politics and society and who had no apparent links to "terrorism." Specifically, the NSA monitored the e-mail addresses of the Council on American-Islamic Relations director Nihad Awad; professors Agha Saeed and Hooshang Amirahmadi; civil rights and defense attorney Asim Ghafoor; and even former Department of Homeland Security staffer and Republican Party operative Faisal Gill. None of these individuals have ever been charged with terrorism-related offenses and Gill holds a top-secret security clearance, as required to work for the DHS.[186] Given that these individuals are U.S. citizens and residents, it is unclear under what authority, if any, the NSA monitored them, as such surveillance would require an individualized court order.

Nonetheless, even where the government used Section 702 spying to collect millions of people's data, the broad categories of non-U.S. persons targeted by the statute necessarily lent legal validity to the mass collection and querying of data pertaining to Muslim communities outside and within the United States.

"Nonetheless, even where the government used Section 702 spying to collect millions of people's data, the broad categories of non-U.S. persons targeted by the statute necessarily lent legal validity to the mass collection and querying of data pertaining to Muslim communities outside and within the United States."

180 - 186 See Appendix

The Trump Era

While Donald Trump and other Republican Party candidates proposed spying on Muslims in the run-up to the 2016 presidential election, and Donald Trump suggested banning Muslims from entering the United States, this rhetorical escalation masked the fact that many of the extreme policies Trump proposed were effectively already in place under the Obama Administration. The Trump Campaign also explicitly called for Muslims to be forced to wear identification for surveillance purposes, that individuals detained as a result of the "War on Terror" be tortured, and that family members of terrorism suspects be killed as a deterrence measure. Upon Trump's assumption of office, several new developments took place.

Black anti-racist protesters are being targeted by the federal government for surveillance and prosecution (Photo: Emmanuel Gido on Unsplash).

Repression of Black Resistance and "Black Identity Extremism"

In 2017, an FBI intelligence assessment was leaked to the public stating that the FBI viewed "Black Identity Extremists" as a potential threat to police officers.[187] Though the vague category of "Black Identity Extremists" was formally abandoned, the FBI nonetheless worked with state and local police departments through the JTTF to spy on Black community activists who protested the rampant police shootings of Black men in the United States and the failure of courts to penalize killer police officers.[188] At the start of the mass rebellion taking place in the United States following the police killing of George Floyd in May 2020, Attorney General William Barr directed the Joint Terrorism Task Forces to target what he called "violent agitators" and "domestic terrorists" based on their "extremist agenda" while police throughout the country brutally cracked down on demonstrators.[189] The Administration's explicit policy justifications for an expansive crackdown are virtually indistinguishable from those offered by the FBI and Army during the COINTELPRO era. At the same time, DHS personnel in Portland, Oregon have surveilled and repeatedly arrested individuals without identification, prompting an outcry from some members of Congress.[190] In one particularly brazen instance of FBI overreach, FBI informants pretending to be members of Hamas, the Gaza-based Islamic Palestinian movement designated as a "foreign terrorist organization" by the U.S. government, manipulated two young men involved in demonstrations against white supremacy and police brutality into contributing weaponry toward what could then be labelled an international terror plot; a Hamas official denounced the sting operation.[191]

Banning Muslims

At the same time, the Trump Administration proposed and implemented multiple versions of his call to ban Muslims. The countries originally targeted under the "Muslim ban" implemented by Trump through an Executive Order were taken from Obama Administration-era order designating Iran, Iraq, Sudan, Syria, Libya, Somalia, and Yemen – all predominantly Muslim countries – as "countries of concern" that would be subject to immigration restrictions.[192] The third version of this ban was upheld by the Supreme Court of the United States in 2018.[193] At the same time, the State Department called for the "extreme vetting" of nationals from six of the countries designated, including searches of social media accounts and biographical and travel information of visa applicants.[194] After years of organizing and mass protests against the Muslim Ban, the House of Representatives attempted to reverse the ban by passing the "NO BAN Act" in 2020.[195] Though the Senate had not yet passed the "NO BAN Act," President Joe Biden repealed the Muslim Ban by executive order in January 2021, on his first day in office.[196]

---

187 - 196 See Appendix

Surveilling Anti-Deportation Efforts

Amid largescale protests against the Trump Administration's restrictive immigration policies, including the separation of children from their parents and the prosecution of undocumented migrants, the Department of Homeland Security began surveilling hundreds of activists and journalists around the country, including their online activity, which was shared with fusion centers.[197] At the same time, Customs and Border Patrol coordinated with the Mexican government to harass journalists and immigration attorneys at the U.S. border crossing between San Diego and Tijuana. This included shackling immigrants' rights advocates to benches in detention, forcing journalists to turn over notes and footage, and photographing their passports.[198]

FISA Limits

Congress re-authorized the NSA's 702 provision without reforms. However, the NSA claims to have ended its "upstream" collection of "about" communications, namely communications in which a selector or target is in the content of the communications between others being searched.[199] The CDR program continued through late 2018 when the NSA suspended it and deleted several years' worth of records; during this time, the NSA continued aggregating significant amounts of data.[200]

More recently, Congress has attempted to renew expiring authorities in the USA PATRIOT Act that had been reauthorized through the USA Freedom Act. H.R. 6172 sought to reauthorize several FISA provisions: one that authorized surveillance against "lone wolf terrorists," another that authorized surveillance on multiple devices and phone numbers when the target is suspected of obtaining a new device or phone number, and a "business records" provision that would not include cell-site location information.[201] The same bill also included some reforms, such as the repeal of the authority for the NSA's Call Detail Records program.[202] However, after opposition to FISA expressed by former President Donald Trump, who blamed abuse of the FISA process for the investigation into his alleged obstruction of justice and collusion with Russia, the renewal lost political support and remains stalled, with those FISA authorities expired.[203]

"Though the Senate had not yet passed the "NO BAN Act," President Joe Biden repealed the Muslim Ban by executive order in January 2021, on his first day in office."

197 - 203 See Appendix

CHAPTER 3

THE LEGAL CONTOURS OF U.S. FEDERAL LAW ON SURVEILLANCE AND RELATED LITIGATION

As the brief sketch of history indicates, much U.S. governmental surveillance has taken place without transparency even among branches of the federal government. As a result of both non-transparency and a general reluctance on the part of the judiciary to challenge the federal government's policies in this realm, existing case law is highly deferential to the federal government and is unfavorable to the communities targeted by the surveillance apparatus. The following section summarizes existing law as it applies to the federal government's surveillance programs and the limits of various types of legal challenges.

First Amendment Challenges to Surveillance

The Laird Barrier

In Laird v. Tatum, 408 U.S. 1 (1972), the U.S. Supreme Court held that a group of civilian activists could not state a claim under the First Amendment against the U.S. Army for a program surveilling civilian political activity (discussed in Chapter 1). The surveillance program in question was carried out during the period of widespread domestic unrest in the late 1960s and early 1970s as Black political movements carried out mass revolts throughout the United States. In an effort to back up local police forces that sought to quell this rebellion, the Army initiated the surveillance program in question, which was largely based on gathering and storing information about activists. Specifically, the Court ruled that where the claim was based on a "subjective chill" effect in which civilians would be less likely to engage in First Amendment protected political activity out of fear that the information gathered from them could be misused in the future, no constitutional violation had occurred. The Laird court distinguished the case from other instances in which surveillance and investigatory authority resulted in unambiguous objective harms to the individuals targeted with surveillance, such as an attorney being disbarred (Baird v. State Bar of Arizona, 401 U.S. 1 (1971)) or a teacher at a public university being fired (Keyishian v. Board of Regents, 385 U.S. 589 (1967)).[204] In short, standing to bring a First Amendment claim requires "a claim of specific present objective harm or a threat of specific future harm." Laird at 19 (citing United Public Workers v. Mitchell, 330 U.S. 75, 89 (1947)). Because the surveillance program in question did not bring with it specific consequences or threats independent of the surveillance program itself, the plaintiffs could not state a claim under this stringent standard. As such, the "subjective chill" on individuals from simply being surveilled, even if it results in hesitancy to engage in political activity, is insufficient to sustain a court action. This leads to particularly jarring conclusions for political dissidents or religious minority groups, including Muslims. Where individuals who find themselves targeted for surveillance in connection with their lawful political activities are already critical of the government, the Laird ruling gives constitutional vindication to the federal government. Combined with AEDPA's repeal of the short-lived federal legislation barring federal authorities from considering First Amendment activity to initiate investigations, the consequence of Laird is that large-scale surveillance databases, protest monitoring, social media trawling, attending of meetings by federal agents, and "voluntary" interviews by federal agents of activists cannot, in and of themselves, be grounds to bring a First Amendment challenge against acts or programs of surveillance. Though the Army compared the surveillance program in question at Laird to the army gathering newspaper clippings from the press, Senate hearings and amicus briefs from intelligence officials who advocated reform indicated that the program was considerably broader, and included the use of plainclothes informants gathering the names of individuals who visited the grave of Martin Luther King, Jr., and the like.[205] A discovery hearing was never held on this matter due to the court's legal conclusion.

204 For a discussion on how First Amendment arguments from some of these other cases might be creatively distinguished and exercised in surveillance cases, see Matthew A. Wasserman, First Amendment Limitations on Police Surveillance: The Case of the Muslim Surveillance Program, 90 N.Y.U. L. Rev. 1786 (2015).

205 Jeffrey L. Vagle, Laird v. Tatum and Article III Standing in Surveillance Cases, 18 U. PA. J. CONST. L. 1055. See also Chapter 1, citing Church Committee Report Book 3 at 800-804.

"The mere existence of surveillance, even when it involves aggressive government intervention in civilian life that targets plainly protected First Amendment activity, is insufficient on its own."

The obstacle to First Amendment claims posed by Laird has stood the test of time. In 2012, the Supreme Court dismissed a lawsuit brought by Amnesty International and other international organizations over the constitutionality of the FISA Amendments Act of 2008. Because the "subjective chill" of the organizations' fear that their communications were likely being surveilled was insufficient under Laird, the organizations could not establish standing to challenge the amended legislation even if it chilled their communications. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 417-419 (2013). The Laird line of cases creates a difficult burden for those who seek to establish First Amendment standing to challenge surveillance. The mere existence of surveillance, even when it involves aggressive government intervention in civilian life that targets plainly protected First Amendment activity, is insufficient on its own.

Overcoming Laird

Despite the formidable barrier created by Laird, some government surveillance has nonetheless created First Amendment standing that has been recognized by the courts. First, litigants have successfully argued for organizational standing where government agents' aggressive surveillance conduct deterred individual members from participation. In Presbyterian Church (USA) vs. United States, 870 F.2d 518 (9th Cir. 1989), the 9th Circuit distinguished a First Amendment claim against government surveillance from the Laird standard where multiple church organizations alleged that their individual members had been subjectively chilled from engaging in worship and church activity as a result of surveillance by immigration enforcement agents. The agents entered church services and electronically recorded the activities of church congregants, apparently in an attempt to detect unlawful conduct related to the sanctuary movement, an effort by clergy to support undocumented migrants fleeing Central America.

When several individuals were later charged for criminal offenses relating to their humanitarian assistance for migrants, the existence of the surveillance was brought up in court and prompted the churches to sue. The court distinguished Laird, stating: "The churches in this case are not claiming simply that the INS surveillance has 'chilled' them from holding worship services.

Rather, they claim that the INS surveillance has chilled individual congregants from attending worship services, and that this effect on the congregants has in turn interfered with the churches' ability to carry out their ministries. The alleged effect on the churches is not a mere subjective chill on their worship activities; it is a concrete, demonstrable decrease in attendance at those worship activities." Presbyterian Church (USA), 870 F.2d at 522 (emphasis in original). The court went on to compare the church's claim for standing with that of the plaintiff in Meese v. Keene, 481 U.S. 465 (1987). In that case, a politician sued over a government designation of films he sponsored as "political propaganda," alleging that the impact on his relationship with the public, which would view him as less reputable, created standing. Because the concrete reduction in attendance similarly affected the churches' ability to engage in their First Amendment-protected religious activity by driving away congregants, the court held that there was standing.[206]

Second, Muslim communities might be able to make a First Amendment Free Exercise claim or Establishment Clause claim. In Hassan v. City of New York, 804 F.3d 277 (3d Cir. 2015), the Third Circuit overruled a district court that dismissed a complaint against the NYPD's Muslim Spying Program for First and Fourteenth Amendment claims.

Specifically, the Circuit held that where a surveillance program is discriminatory, "the indignity of being singled out [by a government] for special burdens on the basis of one's religious calling" was a sufficient injury for standing purposes. Hassan, 804 F.3d at 289 (citing Locke v. Davey, 450 U.S. 712 (2004)). The court rejected the contention that Laird barred suits over surveillance outright, and dismissed the City's arguments that First Amendment Free Exercise claims and Establishment Clause claims required religious animus for standing. The court permitted the plaintiffs to proceed on the merits of their case. Hassan, 804 F.3d at 308. Nonetheless, even where plaintiffs are able to establish standing, other obstacles arise. First, under Wilkie v Robbins, 551 U.S. 547 (2007), where there is an alternative statutory remedy for a constitutional claim, the Judiciary is expected to refrain from finding a constitutional cause of action[207] even

206 In ACLU v. Clapper, 785 F.3d 787 (2d Cir. 2015), the Second Circuit hinted that similar concerns might apply to overbroad NSA bulk metadata collection, before resolving the case on narrower grounds.
207 Such claims are known as "Bivens" suits after Bivens v. Six Unknown Named Agents, 403 U.S. 388 (1971) which found standing for an individual to sue federal agents for constitutional violations absent an explicit statutory grant.

if the statutory remedy does not provide complete relief. For First Amendment claims regarding surveillance, existing federal statutes might therefore replace the Bill of Rights for providing relief. Second, even where there is a valid First Amendment claim, defendants may be able to meet the normally high bar set for restricting speech. Normally, government actions that incidentally restrict speech are subject to "strict scrutiny," meaning that the government must show that the actions serve a compelling interest and are narrowly tailored to effectuating that interest.

Although a plainly discriminatory or politically-motivated surveillance program cannot be said to serve a compelling interest where its explicit goal is to violate constitutional rights, surveillance programs that are plausibly aimed at deterring "terrorism" and other "national security" threats will likely be able to meet the high standard, meaning that plaintiffs will primarily have to focus on whether or not the program is "narrowly tailored." Given the vagueness of the threat posed by "terrorism" and the difficulty in establishing what a "narrowly tailored" program might look like, this may cause additional obstacles for succeeding on a First Amendment claim against surveillance even where standing to sue is established. An additional obstacle exists for immigrant communities, including Muslim immigrant communities. The existing statutory framework under AEDPA and the breadth of the Attorney General's discretion to engage in politically-motivated deportation means that even where immigrant communities are subject to discriminatory surveillance and then deportation, they may not be able to raise First Amendment claims to prevent their deportation. Reno v. American-Arab Anti-Discrimination Comm., 525 U.S. 471 (1999). Note, however, that other types of challenges may still be possible. See, e.g., Iqbal v. Hasty, 490 F.3d 142 (2d Cir. 2007). Likewise, where the First Amendment consequences are particularly severe, some federal courts have drawn conflicting conclusions. See, e.g., Ragbir v. Homan, 923 F.3d 53 (2d Cir. 2019).

The First Amendment and Material Support Prosecutions

A final caveat on the nature of First Amendment protection from surveillance are the post-9/11 restrictions on what types of speech are actually entitled to First Amendment protection at all. Because the Supreme Court has ruled that a speech act, under certain conditions, can itself constitute material support, surveillance based on or aimed at such speech activity will not succeed in obtaining First Amendment protection from surveillance. In Holder v. Humanitarian Law Project, 561 U.S. 1 (2010), the Supreme Court ruled in a declaratory judgment that a human rights organization could not provide legal support to an organization designated as an FTO without running afoul of the statutory ban on material support for "terrorism." That the speech was not directed toward the group's unlawful activities and was in fact part of a campaign to assist the group in conforming to law, and that the assistance in question was an act of speech, did not shield the legal advocacy. The Court reasoned that where the material support statute restricted "only a narrow category of speech to, under the direction of, or in coordination with foreign groups that the speaker knows to be terrorist organizations," no First Amendment violation had taken place. Humanitarian Law Project, 561 U.S. at 26. Citing Humanitarian Law Project, the First Circuit upheld criminal charges against a young Muslim man over his blog posts. In United States v. Mehanna, 735 F.3d 32 (1st Cir. 2013), Tarek Mehanna was charged with material support for "terrorism" in part for pro-Al Qaeda internet posts he had made on the grounds that these posts may have been indirectly coordinated with an agent of Al Qaeda. The breadth of material support charges and their inclusion of speech acts and other forms of traditionally protected political activity thereby further limit the First Amendment protection that individuals may be able to claim where investigations are based on allegedly illegal forms of speech activity with members of an FTO.

Fourth Amendment Challenges to Surveillance

A Reasonable Expectation of Privacy

Because it is the primary source of privacy protections for matters of search and seizure, one might think that the Fourth Amendment of the United States Constitution would provide the primary protection for Muslim communities and others facing mass surveillance. Although the Fourth Amendment provides some protection, there are considerable limits on the scope of Fourth Amendment protection, which are discussed here. The guiding principle of Fourth Amendment jurisdiction is the protection of a person's "reasonable expectation of privacy." In Katz v. United States, 389 U.S. 347 (1967), the Court replaced the trespass standard for the Fourth Amendment and held that the Fourth Amendment applies to any "reasonable expectation of privacy" even when in public and independently of a property standard that would require someone to physically trespass before a violation had taken place. Based on this reading, the Fourth Amendment would no longer be restricted to private property. Rather, any time an individual has a "reasonable expectation of privacy," their privacy interests are at stake and government searches and seizures must conform to the Fourth Amendment, either by obtaining a warrant or establishing an exception to the warrant requirement. Where domestic surveillance is concerned, the Supreme Court has held that the Fourth Amendment applies. United States v. U.S. District Court, 407 U.S. 297 (1972) (herein "Keith").

"It is reasonable to believe, based on the size of the FBI's budget, in conjunction with the broad scope of religious and ethnic mapping that the FBI permits its agents to carry out, that virtually every mosque within the United States can be or has been infiltrated by covert informants as a result."

The Katz case, by jettisoning any sort of physical trespass standard for the Fourth Amendment, ensured that the Fourth Amendment's warrant requirement would extend to wiretapping phones and other electronic surveillance, absent an applicable exception to the Katz rule; however the majority specifically singled out national security cases as a potential exception. Katz, 389 U.S. at 363 n. 30. With regard to domestic electronic surveillance, Congress has passed specific statutory rules that trail the Fourth Amendment's expectations of probable cause and warrant requirements through Title III. Title III requires that police agencies throughout the country obtain a judicially approved warrant prior to engaging in domestic electronic surveillance.

Though this was an expansion to previous Fourth Amendment protections, there are clear limits to the scope of Fourth Amendment protections that nonetheless hamper its usefulness in restricting government surveillance, including the type of government surveillance discussed in this report. The Katz rule does not shield aspects of civilian life that are "public" in some senses but private in others from government surveillance. For example, a political gathering, a religious service, a support group meeting – all intimate spaces involving close personal bonds – are not explicitly protected under the Katz standard where such meetings are open to the public. Indeed, many of the places targeted in sweeping anti-Muslim spying programs such as the municipal program in New York – including Muslim-owned businesses, restaurants, and cafes, Muslim community organizations, Muslim student groups, and mosques, all of which are generally open to the public – are unable to claim protection on Fourth Amendment grounds due to Katz.

The Third Party Doctrine

Moreover, an associated series of rulings that established the so-called "Third Party Doctrine" explicitly permit the gathering of information by undercover government agents under the principle that such information has been voluntarily disclosed to a third party. In United States v. White, 91 S. Ct. 1122 (1971), the Supreme Court held that where an individual is led to disclose information to a covert government informant who holds themselves out as a civilian, an individual has no reasonable expectation of privacy, and therefore no Fourth Amendment violation has taken place. In a similar vein, Smith v. Maryland, 442 U.S. 735 (1979) held that police agents' use of a pen register to log the phone numbers dialed on a particular suspect's phone was not subject to a reasonable expectation of privacy where such information was being freely disclosed to the phone company. In short, where information is divulged either freely to an informant or to another third party, the Fourth Amendment is not violated under the Third Party Doctrine. This restriction is particularly damaging to litigation against mass surveillance, as it signifies that even when covert informants enter spheres that are protected by one's reasonable expectation of privacy on false pretenses, any information divulged to that person is voluntary and not the result of a Fourth Amendment violation. It is reasonable to believe, based on the size of the FBI's budget, in conjunction with the broad scope of religious and ethnic mapping that the FBI permits its agents to carry out, that virtually every mosque within the United States can be or has been infiltrated by covert informants as a result. Furthermore, sensitive documents obtained in the name of "national security," such as bank statements, telephony metadata and the like are not protected by the Fourth Amendment under the rule of Smith because they have been divulged to others. Notably, the Supreme Court has recently issued some restrictions on this rule. In Carpenter v. United States, 138 S. Ct. 2206 (2018), the Supreme Court held that an individual does have a reasonable expectation of privacy in the cellular location data emanating from their phone to cell phone towers.[208]

A number of "carve-outs" exist that create additional exceptions to the protections provided by the Fourth Amendment even where it otherwise applies. For surveillance purposes, the two most relevant exceptions are the foreign intelligence surveillance exception and the border search exception.

The Foreign Intelligence Surveillance Exception

The scope of the ruling in Katz was explicitly limited to cases not "involving the national security." Katz at 358 n. 23. Though the Supreme Court has never explicitly articulated an exception to the warrant requirement for foreign intelligence gathering, this is the implied result of the Court's limited ruling and dictum in Keith. The Court in Keith and the statutory framework of Title III recognized the constitutional authority of the Executive Branch to protect the state from hostile acts of foreign powers, distinguishing this from traditional criminal law enforcement. Keith at 303-304, 309 ("…the instant case requires no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country… the surveillances [in this case involved] attempts of domestic organizations to attack and subvert the existing structure of Government") (emphasis in original). Nonetheless, the Keith court recognized that the national security issues raised in domestic intelligence operations "do not justify complete exemption of domestic security surveillance from prior judicial scrutiny. Official surveillance, whether its purpose be criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy of speech" before holding that domestic intelligence investigations, like criminal investigations, require judicial approval. Keith at 320. The Keith court

208 See Appendix

limited the scope of this ruling to "only the domestic aspects of national security," but recognized that the "standards and procedures described by Title III are not necessarily applicable to [domestic national security surveillance]." Keith at 320. The Court went on to suggest that Congress create guidelines for such forms of investigation distinct from the standards in Title III.

Several years later, in United States v. Truong Dinh Hung, 629 F.2d 908, (4th Cir. 1980), the Fourth Circuit explicitly recognized a "foreign intelligence exception" to the warrant requirement where "the object of the search or the surveillance is a foreign power, its agent or collaborators" and where the search is "primarily for foreign intelligence reasons" as opposed to a criminal investigation.

In the aftermath of the Keith case and the Church Committee findings about domestic spying, Congress passed FISA which created, as suggested by the Keith court, separate standards for foreign intelligence gathering. However, these guidelines were limited only to foreign intelligence, meaning that domestic organizations that are being investigated for "national security" purposes, unless they are believed to be foreign agents, are still subject to Title III rather than FISA. The statutory framework of FISA and its post-9/11 expansion is discussed above. As a result of the expansion, a number of domestic targets which may be subject to FISA surveillance will have difficulty challenging the surveillance, including Muslims accused of being "lone wolf terrorists" and those being tenuously linked to foreign jihadists. However, FISA surveillance can still be challenged successfully where it is the result of blatant and egregious deviations from the statutory framework. See, e.g., ACLU v. Clapper, 785 F.3d 787 (2d Cir. 2015) (holding that the government violated the text of the FISA statute by engaging in bulk data collection); see also United States v. Maolin, No. 12-50572 (9th Cir. 2020) (holding that the government's collection of telephony metadata to be used against a Somali defendant accused of material support offenses violated the FISA statute, but nonetheless refusing to suppress the metadata as evidence based on the court's analysis of other classified disclosures).

The Border Search Exception

The border search exception to the warrant requirement of the Fourth Amendment holds that, as per historical tradition, standard Fourth Amendment protections do not apply to searches in so-called "customs areas" – namely, searches of people at or entering U.S. territory from outside by land, roadway, sea, or air. United States v. Ramsey, 431 U.S. 606 (1977). Under this exception, a warrant is not needed for searches of individuals and their baggage. Some courts have held that where a more intrusive search takes place, such as a body cavity search, some "reasonable suspicion" is required. See, e.g. United States v. Vega-Barvo, 729 F.2d 1341 (11th Cir. 1984).

Above: San Francisco International Airport security personnel Avinash Patel, left, and Armando Gramajo perform a hand search on luggage owned by a passenger, right, Monday, Sept. 17, 2001, in San Francisco. In addition to walking through extra metal detectors, many passengers must hand their bags over for inspection as well. (AP Photo/ Julie Jacobson)

This has a tremendous impact for surveillance purposes, particularly where border officials engage in political, religious, or racial profiling of individuals. For example, in Tabbaa v. Chertoff, 509 F.3d 89 (2d Cir. 2007), the border search exception was used to justify interrogating, photographing, and detaining a group of Muslim men visiting an Islamic religious conference in Canada upon their return, citing secret, unspecified evidence of "terrorism" at the conference. As an extension of the routine border search exception, the men could not challenge this intrusion.[209] This implies that where Muslim community members are targeted for searches and other forms of investigatory action at the border, they may have little relief in court under the Fourth Amendment.

Ethno-Religious Profiling as Probable Cause

One final obstacle encountered by Muslim community members facing surveillance is the question of whether a person's racial or ethnic identity can be a factor supporting probable cause for a search rather than barring a search as unreasonable. Arguing that members of the Muslim and Arab communities are allegedly more likely to be involved in terror attacks, investigators have sometimes attempted to use bigoted stereotyping to justify searches. The courts have not always been helpful. In Whren v. United States, 517 U.S. 806 (1996), the Supreme Court held that where officers pulled over a car on the ostensibly valid grounds of a traffic offense, the fact that the officers may have cited the traffic offense pretextually to justify a stop based on racial discrimination against the driver was irrelevant from a Fourth Amendment perspective. That is, where there is some other justification, discriminatory motives will not invalidate a search: "The Constitution prohibits selective enforcement of the law based on considerations such as race. But the constitutional basis for objecting to intentionally discriminatory application of laws is the Equal Protection Clause, not the Fourth Amendment.

209 The men's First Amendment claim failed on strict scrutiny grounds for similar reasons where the court held that a border search was the "least intrusive" means. Id. at 102-105.

Subjective intentions play no role in ordinary, probable-cause Fourth Amendment analysis." Id. at 813. The Supreme Court has also upheld, in at least one instance, the validity of using ethnic profiling to find that a person may be more likely to be committing a violation. United States v. Brignoni- Ponce, 422 U.S. 873 (1975)(holding that a Mexican appearance was a relevant factor in finding probable cause for immigration stops where a significant percentage of the Mexican-American population is made up of immigrants). Nonetheless, this line of argument has limited application. As the Eastern District of New York noted when facing such arguments during a suit over the detention of two Arab plane passengers in part because of their Arab ethnicity:

> ***No court has ever marshaled statistics to conclude that racial or ethnic appearance is correlated with and thus probative of any type of criminal conduct other than immigration violations… Moreover, the statistical rationale behind the Brignoni-Ponce dictum does not translate to the present case: Even granting that all the participants in the 9/11 attacks were Arabs, and even assuming arguendo that a large proportion of would-be anti-American terrorists are Arabs, the likelihood that any given airline passenger of Arab ethnicity is a terrorist is so negligible that Arab ethnicity has no probative value in a particularized reasonable suspicion or probable cause determination. Farag v. United States, 587 F. Supp. 2d 436 (E.D.N.Y. 2008***
> (emphasis in original).

But given the expansive breadth and highly selective process of prosecuting "terrorism," the danger of depending on such rulings in Fourth Amendment cases is that the federal government could hypothetically create the very statistics that would be necessary to justify using ethnicity as a factor in probable cause determinations by simply targeting Arabs and Muslims for prosecution. Hence, this attempt to limit the creep of bigotry and racist stereotyping into Fourth Amendment jurisprudence is insufficient to ensure strong Fourth Amendment protections.

Equal Protection Claims Under the Fourteenth and Fifth Amendments

The Equal Protection Clause (EPC) of the Fourteenth Amendment is another plausible method of challenging surveillance programs, provided that they are programs that single out a specific community, such as Muslims, Black people, or immigrants, for discriminatory treatment. The substance of an EPC claim is distinct from a Free Exercise claim under the First Amendment.

While the former is based on being unlawfully barred from practicing one's faith, an EPC claim is based on being treated differently because of religious or other specified affiliation. The EPC states, "no State shall…deny to any person within its jurisdiction the equal protection of the laws." An EPC claim can allege intentional discrimination, which includes intentionally targeting a particular community for differential treatment, or discrimination by design, or even the discriminatory application of a facially non-discriminatory law.

The EPC applies to states and municipalities, but not the federal government; however, since Bolling v. Sharpe, 347 U.S. 497 (1954), when the Supreme Court ruled that the Due Process Clause of the Fifth Amendment nonetheless requires the equal protection of the laws itself to strike down racial segregation in the District of Columbia schools, courts have been willing to uphold equal protection claims against the federal government as well. See, e.g., Morrissey v. United States, 871 F.3d 1260, 1272 n. 6 (11th Cir. 2017) ("Although the Fourteenth Amendment's Equal Protection Clause applies by its terms only to the States, the Supreme Court has long recognized that equal protection principles bind the federal government (by what has been termed "reverse incorporation") through the Fifth Amendment's Due Process Clause.").

Intentional Discrimination

Regarding anti-Muslim spying programs such as those that explicitly map out Muslim communities and subject them to differential treatment, Muslim litigants would likely be able to allege intentional discrimination.

The most appropriate case on this matter is Hassan v. City of New York, 804 F.3d 277 (3d Cir. 2015), wherein Muslim groups challenged the municipal Muslim spying program on multiple grounds including the Fourteenth Amendment's Equal Protection Clause.

In finding standing for their claim, the Hassan court considered that the litigants had properly pleaded specific facts about the size and scope of the anti-Muslim spying program to overcome the heightened pleading standards of Ashcroft v. Iqbal, 556 U.S. 662 (2009); that an "invidious motive" is not required for finding discriminatory purpose (citing Snyder v. Louisiana, 552 U.S. 472 (2008) and Bray v. Alexandria Women's Health Clinic, 506 U.S. 263 (1993)); and that intentional religious discrimination is subject to heightened scrutiny that could not be justified without the government showing that their policy was properly tailored. Hassan, 804 F.3d at 295-308.

Notably, the Hassan court considered that there is no Supreme Court holding that expressly extends EPC claims to discrimination based on religion.

However, multiple circuits have addressed the issue and have upheld EPC claims based on religious discrimination, and there is some Supreme Court dicta suggesting so. Specifically, in American Sugar Ref. Co. v. Louisiana, 179 U.S. 89 (1900), the Supreme Court suggested that religious discrimination might be considered an example of denial of equal protection of the laws.

Multiple circuits have explicitly concluded that religious affiliation is a suspect class triggering strict scrutiny. United States v. Brown, 352 F.3d 654, 668 (2d Cir. 2003); Patel v. U.S. Bureau of Prisons, 515 F.3d 807, 816 (8th Cir. 2008); CSRRJM v. San Francisco, 784 F.2d 1010, 1012 (9th Cir. 1986); Abdulhaseeb v. Calbone, 600 F.3d 1301, 1322 n.10 (10th Cir. 2010).

As such, there is overwhelming authority to establish that discrimination targeting religious affiliation is enough to state a Fourteenth Amendment claim subject to heightened scrutiny.

Discriminatory Application of Facially Neutral Laws

Communities targeted with discrimination can also allege EPC claims based on the discriminatory application of facially neutral laws. Under such a claim, the government has violated the EPC where it has administered a neutral ordinance "with a mind so unequal and oppressive as to amount to a practical denial by the State of that equal protection of the laws." Yick Wo v. Hopkins, 118 U.S. 356 (1886).

One of the most emblematic recent successes against a widespread campaign of ethnic profiling on this basis was the Second Circuit's ruling in Floyd v. City of New York, 959 F. Supp. 2d 540 (2013). In Floyd, Black and Latinx plaintiffs challenged the NYPD's program of applying a facially neutral policy of stopping and frisking individuals on the streets of New York in a racially discriminatory manner.

While such a policy is not perfectly analogous to programmatic surveillance, the interplay of discriminatory profiling and police investigation make it apt as a model for bringing EPC claims.

To succeed in Floyd, plaintiffs had to prove not only the existence of a disparate impact on Black and Latinx communities as a result of the stops, but that discriminatory intent was responsible for this impact, where defendants applied their policy in part for discriminatory reasons. Floyd, 959 F. Supp. 2d at 661-662.

Where the NYPD admitted it was targeting Black and Latinx men based on the claim that these groups were more heavily represented in crime data, the court held that the discriminatory application of facially neutral policy had taken place. Id. Where relevant information exists that government agencies are using similar justifications to engage in searches against Muslim individuals or groups, a similar complaint might be put forward.

The State Secrets Hurdle

In addition to the various litigation hurdles and obstacles plaintiffs in surveillance litigation must overcome in specific areas of law, all federal surveillance-related civil litigation is likely to face the state secrets privilege hurdle.

The state secrets privilege is an evidentiary privilege that allows the federal government to block the release of information demanded during litigation on the grounds that the release would damage "national security." U.S. v. Reynolds, 345 U.S. 1, 10 (1953).

Some circuit courts have held that where the government has properly withheld information under the privilege that is essential to the plaintiff's claim, the lawsuit cannot go forward, including some claims by survivors of the Extraordinary Renditions program. El-Masri v. United States, 479 F.3d 296 (4th Cir. 2007); Mohamed v. Jeppesen Dataplan, Inc., 614 F.3d 1070 (9th Cir. 2010).[210]

Nonetheless, where a Congressional statute governs the process of releasing information, that statute's rules displace the rules of the state secrets privilege. For example, in Fazaga v. FBI, 916 F.3d 1202 (9th Cir. 2019), the Ninth Circuit ruled that where a claim was governed by FISA, the statutory framework displaces the state secrets privilege as the governing rule.

210 See Appendix

CHAPTER 4

SURVEILLANCE BY :
STATE AND LOCAL AGENCIES

State and municipal agencies are central to the overarching surveillance apparatus. Much of the federal government's surveillance efforts are closely coordinated with state governments. In fact, the federal government has never had a monopoly on mass surveillance efforts. Throughout the Cold War era, local police departments themselves adopted their own surveillance programs which similarly targeted directly-impacted communities and political dissenters.[211]

In the post-9/11 era, the most notorious example of municipal spying was the NYPD's Muslim Surveillance Program, discussed above. But the reality is that the NYPD is not alone or unique. Throughout the U.S. South, state agencies and municipalities have adopted spying efforts and policies, often in coordination with the federal government and other agencies, that have placed Muslim communities and others in a place of suspicion and risk.

This chapter discusses state surveillance targeting Muslims and others in five Southern states: Georgia, North Carolina, Florida, Louisiana, and South Carolina. The information here has been gathered through multiple sources: existing information compiled by community organizations and journalists; records requests through federal and state freedom of information laws; and community outreach in the states in question.

The picture that emerges should make clear that federal agencies are not the only agencies responsible for unjustified spying and that local and state agencies are also engaged in policies that are likely targeting Muslims, usually in close coordination with federal agencies.

211 See Donner, supra note 16.

"In the post-9/11 era, the most notorious example of municipal spying was the NYPD's Muslim Surveillance Program, discussed to the left. But the reality is that the NYPD is not alone or unique. Throughout the U.S. South, state agencies and municipalities have adopted spying efforts and policies, often in coordination with the federal government and other agencies, that have placed Muslim communities and others in a place of suspicion and risk."

GEORGIA

In Georgia, local and state officials have primarily engaged in harmful surveillance practices through two means: the use of a state-run fusion center known as the Georgia Information Sharing and Analysis Center, and through the FBI-run Joint Terrorism Task Force.

Expansive Surveillance Guidelines at the Georgia Bureau of Investigation & GISAC Fusion Center

The Georgia Bureau of Investigation is Georgia's state-level investigative agency. The GBI maintains multiple criminal information databases and also operates the Georgia Information Sharing and Analysis Center (GISAC). GISAC is a fusion center used by the GBI and authorized collaborating local agencies to store both information that may be relevant to a criminal investigation as well as "suspicious activity reports" or SARs. In response to an Open Records Request by Project South, GBI released to Project South a number of documents regarding GISAC, several of which are discussed below.

Internal audits released by the GBI to Project South indicate that the GBI regularly ensures that outside auditors, along with a designated GBI Privacy Officer, guarantee that information stored in GISAC conforms to both state legislation and overarching investigative guidelines set by the GBI. GBI also has implemented procedures limiting the authority of GBI investigators to monitor public social media posts. The problem, however, is that the statutes themselves do not provide sufficient protection to ensure that the GBI is not cataloguing sensitive information pertaining to Muslim community members and others. While GBI's implementation of some restrictions on their officers' social media monitoring and the existence of some guidelines to ensure limits to storing sensitive information on GISAC should be welcome, the lack of complete transparency and the weakness of the governing statute leave considerable room for concern.

Directive 7-6: Overarching Intelligence Gathering Guidelines

Directive 7-6 is the document that governs GBI's gathering and retention of data with respect to individual privacy. Because GISAC is operated by the GBI, the directive also governs GISAC. The privacy protections listed in Directive 7-6 are problematic for a number of reasons. First, the requirements for what type of "criminal intelligence information" will be sought or retained by GISAC include at least one category that is not limited by the reasonable suspicion or probable cause requirements. GISAC is authorized to gather information that is "relevant" to investigating and prosecuting crime, to enforcing penalties, and to "the prevention of crime."[212] The "relevance" standard untethers GISAC from the limits of the Fourth Amendment and appears to permit GISAC to gather evidence from people who are not engaged in criminal activity. Because "relevance" also pertains to the prevention of crime, this limit also appears to enable storing information for the purpose of preemptive and anticipatory prosecutions. Second, Directive 7-6 provides a weak restraint on gathering evidence against people based on a protected characteristic. Directive 7-6 bars the GBI from seeking or retaining information about individuals "solely" because of their religious, political, or social views, or activities.[213]

While targeting people for their "religious" views or activities are listed under the "solely" subcategory, GBI separately states that it will not seek or retain information about a person's race, ethnicity, citizenship, place of origin, age, disability, gender or sexual orientation, or their participation in a particular non-criminal organization or lawful event. Conspicuously missing is "religion." This would indicate that the GBI and GISAC could gather information on Muslims, provided that the surveillance is not "solely" based on religious views. Indeed, in separate documents released to Project South by the Georgia Emergency Management and Homeland Security agency, e-mails between GEMA-HS staff and the GBI indicated that the organizations were monitoring Black Lives Matter demonstrations for "situational awareness" purposes, indicating the ease with which GBI could circumvent the "solely" restriction. The "Analysis and Merging" section of the policy indicates that GBI analysts will be tasked with analyzing the data to engage in "further crime prevention" including "terrorism" or to "provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal activities."[214] All of these aspects of the policy, taken together, suggest that the GBI would be able to surveil Muslim community members on flimsy pretexts without any indicator of criminal activity. Separate from the criminal intelligence information is the way GISAC maintains suspicious activity reports, or SARs. SARs are reviewed by GISAC analysts to make sure that they comply with the National Security Initiative (NSI) list of indicators that suggest a potential nexus to "terrorism" before entering them into the FBI's SAR database, known as eGuardian. However, the list of indicators published by NSI includes not only a list of criminal activities that may or may not have anything to do with "terrorism" (such as false documents), but also a second series of both criminal and non-criminal activities that, according to NSI, require "additional information during vetting" such as taking photos of facilities or gaining expertise in security concepts.[215] GISAC technicians must ensure that SARs are "reasonably indicative of behaviors related to preoperational planning related to terrorism or other criminal activity" (emphasis added).[216] Non-"terrorism"-related information that indicates

212 - 216 See Appendix

criminal activity is forwarded to local law enforcement, while "terrorism"-related SARs are maintained for five years on the FBI- run eGuardian system. SARs must be investigated within 90 days to determine if they are of any value. Because this standard is not about "terrorism" per se but suspected "preoperational planning," and includes non-"terrorism"-related criminal activity, this category is broad.[217] Though GBI and GISAC maintain a method for the public to register complaints, there is no way members of the public would know that they are being spied on or that their information is being collected.

Directive 8-6-5: Social Media Guidelines
Directive 8-6-5 governs GBI's use of social media. Here, the standards for data gathering and retention are even lower. In addition to the "relevance" standard, the directive permits data gathering for information as well as creating an online alias to gather information that is "useful in crime analysis or situational assessment reports."[218]
Regarding protected characteristics, directive 8-6-5 is virtually identical to the standard in Directive 7-6. The policy explicitly permits agents to make false representations to conceal their identities. Although there is a lengthy documentary and approval process for agents to use social media, an "exigent circumstances" exception mimicking the authority abused by the FBI (discussed in Chapter 2) permits the agents to monitor social media through verbal authorization.[219] The directive explicitly permits the monitoring of "First Amendment-protected activities" for the purpose of "crime analysis and situational assessment reports."[220] The data is to be purged within 14 days unless there is a criminal nexus. Additionally, a section detailing "Off Duty Conduct" permits off duty agents to monitor potential criminal activity simply by coordinating with their supervisor or CEACC (Child Exploitation And Computer Crimes unit) "if the activity involves a minor child or exigent circumstances to determine the best course of action" and requires them to detail the encounter "as soon as practical."[221]

Directive 8-8-23: Facial Recognition Software Guidelines
This document, included as part of GISAC's 2017 privacy report, summarizes the weak privacy protections the GBI applies to its use of facial recognition data in its criminal intelligence surveillance. The document states that the GBI "does not maintain or operate any system that utilizes face recognition software or technology. The GBI also does not perform any face scans of the public for face recognition purposes. Finally, the GBI does not employ any persons trained to perform manual face examinations of a probe photograph with a candidate photograph(s)."[222]

However, the document also states that employees may "make a request for the use of face recognition software to the Georgia Department of Driver Services (GA DDS) Investigative Division or to out-of-state law enforcement agencies/ fusion centers" in accordance with the policy directive.[223]
The directive permits agents to request the use of facial recognition software for several reasons, one of which is "criminal intelligence development."[224] The directive states that GBI employees can request facial recognition software according to the "relevance" standard, alongside reasonable suspicion and criminal predicate standards. In barring the use of facial recognition standard, the policy again uses the "solely" directive as pertaining to characteristics such as race.[225] Retention of this information is governed by relevant law depending on the purpose for gathering the information.

Annual Privacy Presentations
Each annual privacy report provided to Project South includes a copy of the privacy presentations given to agents. The 2014 presentation deals with police officers posting embarrassing information on social media or e-mail. The 2015 presentation goes through a series of topics, only some of which are related to surveillance, such as evolving legal precedents relating to car stops.
The 2016 presentation focuses heavily on privacy rights and details the public's increasing outrage and distrust of police officers due to surveillance. The presentation suggests that due to the lack of clear legal guidelines for surveillance and the use of new technologies, the agency has implemented its own "rigid guidelines," pointing to the directives established. It briefly touches on the 2014 IACP Guidelines for new technology use by law enforcement and includes several examples of overreach, including license plate readers that were abandoned by Tybee police amid protests. Notably, the guidelines appear to suggest that public outrage is one of the limits to acceptable surveillance that the GBI pays attention to – despite the fact that much of what GBI agents do is not revealed to the public.
The 2017 privacy presentation covers "emerging technology" and deals with the public's outrage over various technologies that were implemented, such as license plate readers. It emphasizes the importance of the purpose for using new technology in order to ensure no overreach.

Privacy Audits
Each annual report includes a privacy audit memorandum. This is an outside annual audit of GISAC and associated offices for compliance with relevant directives. Each audit is a checklist for compliance with the policies in question filled out by the Privacy Officer along with various outside officers. Included are audits that describe particular SARs and reports that were selected at random to establish compliance. All reports indicate that GISAC is in compliance. However, the actual SARs and reports selected themselves are not included. Furthermore,

217 - 225 See Appendix

given the problematic nature of the guidelines, it is not clear that compliance with the Directives necessarily indicates lawful or non-discriminatory use.

Conclusions about GBI & GISAC

The picture that emerges from GBI's own records suggests that the GBI is using many of the same flawed "safeguards" as the FBI, which permit agents to target a broad swath of people under both a "criminal intelligence" predicate and SAR predicate. Those flawed safeguards permit data gathering when it is "relevant" or "useful" to a criminal investigation. This includes non-criminal information gathered to paint a comprehensive "threat picture," so long as it satisfies the "mere suspicion" standard. It also permits gathering information pertaining to race and religious and political views, provided the information is not gathered "solely" due to these reasons. Additionally, that GISAC's SAR system is designed to work with eGuardian indicates that the GBI does share the intelligence with the FBI through GISAC.

In addition, much of the agency's privacy trainings appear to be primarily about balancing the use of technology and surveillance against the public's outrage. The problem is that the use of these technologies is rarely revealed to the public and the exact nature and scope of GISAC remains unclear. Hence, the disclosures give the subtle indication that the GBI and GISAC can do what they please within a shaky system of guidelines provided that the public never finds out or, if they do find out, that there is not significant political backlash.

While we have not seen documentation so far indicating that the GBI is systematically targeting Muslim communities or engaging in geo-mapping as in the NYPD case, the legal framework is loose enough for them to do exactly that using the "relevant," "useful," and "solely" standards.

Federal-to-Local Spying and Prosecution

JTTF & Pentagon Monitoring Protest Activity

GISAC and other Georgia police departments are open about their collaboration with the FBI; much of the surveillance that has taken place in Georgia has in fact been directed by the federal government. Some of the more notable instances of government surveillance in recent decades were aimed at animal rights activists and anti-war protesters.

In 2006, the ACLU filed multiple freedom of information requests with the Department of Defense over media reports of federal spying on anti-war demonstrators. The disclosures revealed that the Pentagon had been documenting the views and activities of numerous anti-war groups throughout the United States, including in the U.S. South, through a program known as "TALON" a program and database system initiated in 2003 by former Deputy Secretary of Defense Paul Wolfowitz. In Georgia, the Pentagon was keeping extensive tabs on the Georgia Peace and Justice Coalition, the International Action Center, Students for Peace and Justice, Iraq Veterans Against the War, and Military Families Speak Out, and continued to keep data pertaining to their activities and protests even where the Department of Defense determined that there was no credible threat of "terrorism."[226] At the same time, an ACLU records request revealed that the FBI's Joint Terrorism Task Force had been aggressively gathering information on the School of Americas Watch, a coalition dedicated to protesting the training of right-wing paramilitaries from Latin America at the School of the Americas at Fort Benning, alongside others.[227] Much like the spying on CISPES throughout the 1980s, these individuals were tracked, their political events logged, and their names put into various databases.

Preemptive Prosecutions of Shifa Sadequee & Syed Harris Ahmed

At the same time, the FBI reserved particularly abusive surveillance practices for several Georgia Muslims, culminating in major prosecutions aimed at Atlanta-area Muslim teenagers Elhasun "Shifa" Sadequee and Syed Harris Ahmed. While the Sadequee and Ahmed prosecutions follow the pattern of turning apparently legal conduct and political speech into evidence of criminal activity, what is notable about the prosecution was the extent to which federal agents surveilled the two youths and others in the immediate run-up to their arrests in order to gather such information.

Ahmed and Sadequee, both young Muslims living in Georgia, first came to the attention of the JTTF when they were identified as associates of a number of Muslims targeted for prosecution in Toronto. The individuals targeted in the Toronto prosecutions were Muslim men who discussed their religious and political beliefs, met together for camping in Toronto, and discussed, but did not plan, illegal activities.[228] While those prosecutions, handled by Canadian authorities, were mostly dropped, Ahmed and Sadequee came to the JTTF's attention.

Above: Shifa Sadequee (S. Sadequee).

After establishing that Sadequee and Ahmed were online associates of those targeted in Canada, JTTF agents used

226 - 228 See Appendix

FISA-approved surveillance to infiltrate an online community to which both men belonged and to gather their online communications, monitoring the men's translations of religious documents and political discussions. While some of the political discussion mentioned violence and war, there was no indication that the individuals in the chat room were actually planning any violent activity. Likewise, though both men had traveled to Washington D.C., and separately to Pakistan and Bangladesh, no evidence indicated that either individual had actually attempted to work with, train with, or otherwise join any proscribed organizations. Rather, when prosecuting both Ahmed and Sadequee, the government admitted that the case was based on the expansive material support laws and federal statutory framework discussed in Chapter 2.[229]

Instead, having infiltrated and surveilled Sadequee and Ahmed's online community, the prosecutors were able to portray a series of online discussions and chats in which the men fantasized about war with the U.S. government amidst other discussions related to Islam and politics to suggest that the men were conspiring to support "terrorism." Notably, in Sadequee's case, the prosecution approached the outer rungs of accomplice liability: "the defendant is charged with conspiring with others to provide material support for some plan, some conspiracy, to commit violent acts abroad or in the United States."[230] Alongside these chats, the prosecution argued that Sadequee and Ahmed's video recordings of landmarks in the United States, later provided to other individuals that the government alleges to be affiliated with terrorism, constituted "material support," despite acknowledging that the videos provided no actual value for the purpose of terror attacks. Likewise, the two men's travels abroad, none of which resulted in either attending any training camps or military activities, were alleged by the prosecution to be attempts at providing themselves as personnel, a form of material support. Notably, the prosecution claimed that the men's decision to engage in a paintball game, which the government conceded was "an otherwise innocent activity," indicated that the men were planning to train themselves as armed personnel for the purpose of terrorism.[231]

In defending himself, Sadequee noted that had he or Ahmed been interested in traveling to Bangladesh and Pakistan for the purpose of attending militant training camps, doing so would have been relatively easy given that some of the organizations they were alleged to be supporting were accessible by phone and that the government itself alleged that they had extensive contacts with those involved in the proscribed organizations.[232] Rather, he pointed out that he and Ahmed had traveled for entirely benign reasons such as visiting family, getting married, and studying. Nonetheless, Sadequee and Harris were convicted of four counts of "terrorism"-related charges. Both the expansiveness of the application of the counter-"terrorism" statutes and the extent to which the JTTF agents were able to surveil Sadequee and Harris' most intimate political and religious communications as a function of the national security framework indicate the overreach of the government's intelligence-gathering. While the surveillance and prosecution of Sadequee and Harris were extreme on their own, other notable aspects of the case were the government's collaboration with the Bangladeshi government in kidnapping and then rendering Sadequee to the United States,[233] and keeping Sadequee in solitary confinement for the entirety of his pre-trial detention, lasting 1,300 days, itself arguably a form of torture.[234]

Recent Incidents

Of course, not all surveillance in Georgia has led to such dramatic prosecutions. Nonetheless, federal and local authorities in Georgia continue to engage in practices toward Muslim community members that indicate mass surveillance, using the permissive legal frameworks described in Chapter 2. Project South has received several reports from Muslim immigrants who were approached in their homes for questioning by federal agents within the last few years. All of those visited were non-citizens, placing them in the difficult and dangerous position of being pressured to divulge information that may risk exposing themselves to potential immigration consequences.

Project South has confirmed at least one instance in which a U.S.-citizen Muslim youth who is actively involved in grassroots political causes was approached by officers from both the Cobb County Police Department and the FBI at his home, indicating that it was likely a JTTF investigation. During that encounter, the officers interrogated him about his social media posts, his political views, and whether or not he believes in political violence. Nothing he had written online indicated anything other than lawful political activities and discussion. While his political activities were not directly related to the Islamic faith or the Muslim community per se, he has an identifiably Muslim name and he believes, based on speaking with others involved in the same organizations, that he was the only individual in the grassroots community organizations who was monitored and approached.

The operations of the GBI, including GISAC with its flimsy "safeguards," as well as the GBI's open collaboration with the FBI make clear that federal surveillance mechanisms are not the only ones at play in states like Georgia. Baseless preemptive prosecutions and unprompted, targeted questioning of Muslims indicate state authorities are also engaging in mass surveillance tactics against members of local Muslim communities. Evidence of the implementation of a number of similar tactics in other states in the U.S. South indicates the same.

229 - 234 See Appendix

NORTH CAROLINA

Surveillance in North Carolina is characterized by two notable phenomena: the extensive use and abuse of surveillance technology on the one hand, and the secrecy and lack of transparency with which the state of North Carolina government is able to use it with on the other. Of the states surveyed by Project South, North Carolina has the most restrictive freedom of information law, allowing North Carolina state and local agencies to conceal much of the information that would otherwise be available to researchers and civil rights activists.

North Carolina's public records law excludes from the definition of "public records" any "records of criminal investigations conducted by public law enforcement agencies [and] records of criminal intelligence information compiled by public law enforcement agencies."[235] An even more expansive exclusion is the law's "sensitive public security information" exclusion, which defines public records to exclude " information containing specific details of public security plans and arrangements or the detailed plans and drawings of public buildings and infrastructure facilities or plans, schedules, or other documents that include information regarding patterns or practices associated with executive protection and security" and "specific security information or detailed plans, patterns, or practices to prevent or respond to criminal, gang, or organized illegal activity."[236]

Of the local and state departments from which Project South requested records, virtually all cited the law's exemptions and did not turn over any of the information requested, with the exceptions of the Chapel Hill Police Department, which provided some policy documentation, and the State Bureau of Investigation, which provided background information on the state's fusion center.

At the same time, there is no ambiguity about the fact that North Carolina authorities have embraced surveillance aggressively. In efforts to uncover the kinds of technology at work in North Carolina, the ACLU of North Carolina found that police departments throughout the state were using license plate readers, cell phone location tracking, surveillance cameras, and drones to log and store data without any oversight or meaningful regulation.[237] Likewise, North Carolina has had twenty-five terrorism-related prosecutions since 2001, the vast majority of cases involving the use of informants.[238]

Expansive Surveillance Guidelines at the State Bureau of Investigation & NCISAAC

North Carolina's state-run fusion center, the North Carolina Information Sharing and Analysis Center (NCISAAC), is run by the State Bureau of Investigation. Information gathered through NCISAAC is shared with other North Carolina state police entities as well as the FBI and the Department of Homeland Security, depending on the nature of the information gathered.
Documents released to Project South discussing the internal structure of the State Bureau of Investigation's storage of intelligence information on NCISAAC reveal, as with other intelligence gathering campaigns, a stark contrast between the way agencies store "criminal intelligence" information, which is tethered to standard Fourth Amendment requirements of reasonable suspicion and probable cause, and "suspicious activity reports."[239] Notably, NCISAAC's criminal intelligence information guidelines uses the "merely"/"solely" standard regarding information gathered "due to political or religious affiliation, or race or ethnicity."[240] Regarding "suspicious activity reports," however, NCISAAC permits the gathering of any information that is "relevant to an investigation," including a terrorism investigation, that is "useful" to an investigation, or that "was collected in a fair and lawful manner." Information gathered may be information based on "less than reasonable suspicion" and will be shared with the FBI's eGuardian system.[241]

A joint NCISAAC and Department of Homeland Security report obtained by The Intercept in 2016 sheds some light on the way NCISAAC views its role of providing situational awareness.
The six-page report documents the rise of some low-level acts of vandalism and other crimes in the aftermath of Donald Trump's election and suggests a correlation between the election results and such acts. But, as Mike German, a former FBI intelligence agent, explains, the report does not appear to actually provide any useful information for law enforcement purposes. Rather, the report appears to suggest simply that NCISAAC and DHS view political motives as indicative or causal of criminality.[242]
Local police departments have not fared much better. Though some departments have limits on what sort of information their officers can gather, others do not appear to have any meaningful policy limits at all. For example, University of North Carolina at Chapel Hill's dedicated police department used covert informants to infiltrate student-led protests against a campus confederate monument.[243]
The North Carolina General Assembly Police, in conjunction with the Raleigh Police Department, also used plainclothes informants to infiltrate the Moral Mondays social justice movement's non-violent demonstrations at the North Carolina state legislature, prompting concern from civil liberties advocates and the local NAACP.[244] Notably, this infiltration not only included attending protests, but also organizational meetings that the Moral Mondays demonstrators had set up, supposedly to gauge what police resources would be necessary in the event of planned acts of non-violent civil disobedience.

---

235 - 244 See Appendix

Federal-to-Local Spying and Prosecution

The JTTF-led Targeting and Prosecution of the Raleigh 7

As with other states, much of the aggressive surveillance carried out by state and federal authorities has been aimed at Muslim youth and has involved questionable intelligence tactics and interpretations of both counter-terrorism statutes and the youths' beliefs themselves. Overall, the FBI and North Carolina authorities have prosecuted twenty-five people, virtually all of them Muslim, for vague terrorism-related crimes.[245] Such was the prosecution of Ziyad Yaghi, one of several young Muslims from the Raleigh area who were ensnared by an overzealous JTTF investigation that suggested that the young men were "terrorists" over their political and religious beliefs. Yaghi and his co-defendants became known as the Raleigh 7. The investigation into the Raleigh 7 was carried out by the JTTF in coordination with NCISAAC as well as the Durham Police Department, the North Carolina State Bureau of Investigation, the North Carolina Department of Public Safety, and the Department of Homeland Security.[246]

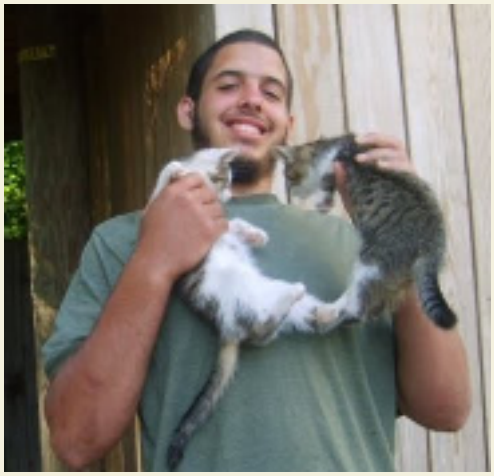
Yaghi's prosecution is notable for several reasons: the fact that Yaghi and several other defendants had no actual ties or relationships with any alleged "terrorist" groups; that his conviction was based almost entirely on their political and religious speech; and that, despite Yaghi being a U.S. citizen with no apparent ties to foreign states or foreign "terrorist" organizations, Yaghi's communications were subject to a FISA warrant on the basis that he was a "foreign agent."

In 2006, Yaghi met Daniel Boyd, a Muslim convert and elder, in a Raleigh-area mosque. Enchanted by Boyd's claims that he had been involved in the Mujahadeen insurgency against the Soviet invasion of Afghanistan in the 1980s, Yaghi and Boyd began a brief friendship. Yaghi and other young Muslims would visit Boyd at his home to discuss politics and their shared religious beliefs.

Around this time, the FISA Court approved of subjecting Yaghi to a wiretap for reasons that have never been disclosed. Though Yaghi expressed violent political views in person and online, there was no indication that he had actually committed or was in the process of planning to commit any crime, or that he was acting as anyone's agent.

In 2006, Yaghi traveled to Jordan to meet with relatives. During this time, he e-mailed Boyd for recommendations about reputable Islamic schools and scholars whom he could contact for the purpose of studying. Yaghi also considered marrying a Jordanian woman, a topic he mentioned to Boyd. After returning from the trip, Yaghi's friendship with Boyd continued, and Yaghi brought additional friends, such as Omar Ali Hassan, to Boyd's home. In 2007, Yaghi and Hassan sought to accompany Boyd on a family trip to Palestine. Because the trip was for family, Boyd instead offered to buy Yaghi and Hassan tickets separately. Yaghi and Hassan were not permitted to enter the Israeli-occupied Palestinian Territories, however, as per the Israeli government's well-established discriminatory border policies against Arabs and those of Palestinian ancestry like Yaghi. Instead, the two men traveled to Jordan. After their trip, Yaghi continued occasionally meeting with Boyd, and introduced Boyd to additional young Muslims. In 2009, Yaghi, Boyd, Hassan, and four others were arrested by the Joint Terrorism Task Force and accused of varying counts of terrorism-related offenses. Boyd and several other defendants were accused of additional non-terrorism related offenses. At trial, Boyd and his sons agreed to testify against Yaghi and others in exchange for a lower sentence. The government also introduced a questionable "terrorism expert" who suggested, without any empirical data to back his methodology, that Yaghi and the other defendants had the characteristics of radicalized "terrorists."[247] The prosecutors suggested that Yaghi's decision to bring his friends to Boyd's home constituted providing personnel to a "terrorist" conspiracy, and that the various trips abroad were attempts to carry out the conspiracy by trying to unsuccessfully engage in terrorism.

Below: Ziyad Yaghi (Project Salam).



At trial, the government heavily emphasized Yaghi's political and religious views, introducing, among other pieces of evidence, his speeches at a Raleigh community mosque discussing jihad, the views he shared with Boyd about armed resistance, and violent rap lyrics he had posted on social media. While none of these individual acts of speech constituted a crime, the federal government introduced them as evidence that Yaghi had entered into a conspiracy with Boyd to engage in material support for terrorism. At no point was Yaghi linked to any actual "terrorist" organization. Furthermore, the evidence that Yaghi was pursuing terrorism was limited to insinuations that his communications with Boyd about looking for Islamic scholars or marrying a Jordanian woman were coded messages about making terrorism-related contacts. Additionally, the questionable terrorism expert's highly prejudicial testimony was sustained by both the trial court and an appeals court.[248]

245 - 248 See Appendix

Yaghi also tried challenging the government's decision to surveil him as a foreign agent. But at both the trial level and the appellate level, the court carried out an in camera and ex parte review of the FISA warrant, barring Yaghi or his attorneys from seeing the basis.[249] While both courts ruled that Yaghi was a foreign agent, the reality remains that the FISA order was granted long before Yaghi made any overseas trips and without any indication that he ever contacted anyone connected to terrorism. Rather, the conspiracy charges against Yaghi depended on considering the "global jihad movement" a single criminal conspiracy. Thus, it is likely that Yaghi was considered an agent of this "conspiracy" based on his political and religious statements.

With little more than the expression of violent political views but no apparent action, the JTTF was able to surveil Yaghi's communications, and these communications, even when innocent, were enough in government's eyes to create an elaborate conspiracy to violate the material support statutes. Yaghi was ultimately convicted and sentenced to over thirty-one years in prison. Yaghi's co-defendants, other young Muslims who were prosecuted in a similar manner, did not fare much better. Omar Ali Hassan received fifteen years in prison.

Recent Incidents

Though the prosecution of Yaghi and the Raleigh 7 took place over a decade ago, Project South has been able to establish through its community contacts that harassment and questionable surveillance policies from the JTTF continue. First, Muslims, particularly Muslim leadership, have been repeatedly visited by federal authorities. These authorities have asked them to serve as informants and to report "suspicious activity." In addition, Muslims who are involved in political activity report received unwelcome visits by federal agents. The individuals who have reported to Project South that they have been approached in such a manner are from immigrant and/or Black backgrounds.

FLORIDA

Of the states researched by Project South, Florida has the highest number of terrorism-related prosecutions at seventy-five.[250] Florida also operates two different fusion centers and has an active and aggressive FBI presence that has carried out numerous abusive prosecutions collaborating with state and local authorities and using aggressive surveillance practices. In a particularly disturbing recent incident, the University of Miami Police Department used facial recognition software to identify and discipline campus protesters challenging the school's reopening during the COVID-19 pandemic.[251] In fact, as this section demonstrates, such incidents of coordinated spying against dissidents have a lengthy recent history in Florida.

Fusion Centers: SEFFC and the Florida Fusion Center

Florida has two primary fusion centers: the Florida Fusion Center (FFC) and the Southeast Florida Fusion Center (SEFFC), which is also the Miami-Dade Police Department's Homeland Security Bureau.[252] Both Florida fusion centers have policies that permit the gathering of data without being tethered to reasonable suspicion or probable cause, as we have seen with other fusion centers. Both the FFC and the SEFFC permit the storage of information that is "based upon reasonable suspicion that the information constitutes a credible criminal predicate or a potential threat to public safety" as well as information that is "based upon reasonable suspicion" that someone is committing a crime.[253] However, the SEFFC policy also permits gathering information "based upon reasonable suspicion" that someone wants to engage in "activity that presents a threat to any individual, the community or the nation" or "is relevant to an active or ongoing investigation…or the prevention of crime reasonably believed likely to occur without such preventative effort."[254] The SEFFC policy also states that the SEFFC will retain information that is "useful in crime analysis or in the administration of criminal justice and public safety" and information "that was collected in a fair and lawful manner not otherwise prohibited by law."[255] Finally, both fusion centers use the familiar overly narrowing term "solely" with regard to collecting information related to someone's protected characteristics, enabling profiling and ethnic mapping.[256]

Federal-to-Local Spying and Prosecution

Fusion Centers and JTTF Target Muslim Teens

The fusion centers have been active in JTTF prosecutions, including at least one in which two men originally came to the attention of authorities for their prayer practices and political views.[257] In that case, Raees Alam Qazi and his brother Sheheryar Alam Qazi were targeted in an FBI sting operation after Raees, then seventeen years old, was pulled aside in the Miami International Airport when he was praying. An FBI agent asked him about his beliefs and political views and began monitoring him before another FBI agent pretending to be a violent extremist tricked him and his brother into joining a violent terror plot.[258]

249 - 258 See Appendix

The Collapse of the FISA Wall: The Prosecution of Sami Al-Arian

Dr. Sami Al-Arian, a former University of South Florida tenured professor and Palestinian immigrant, had been politically active in the United States for many years, seeking to defend the civil rights of Muslim-Americans. As early as 1993, however, the U.S. government began spying on him through the FISA system on the basis that he may have been an agent of the Palestinian Islamic Jihad, a Palestinian organization that the United States has designated as an FTO. While the surveillance had been ongoing, no charges were brought, likely owing to the "wall" between foreign intelligence gathering and criminal prosecution discussed in Chapters 1 and 2 above.[259]

Above: Dr. Al-Arian and his family. (Courtesy L. Al-Arian)

In the aftermath of the September 11th attacks, however, circumstances enabled federal prosecutors and the JTTF to charge Dr. Al-Arian with "terrorism"-related offenses. After a tumultuous interview with a right-wing talk show host in the weeks after the September 11th attacks triggered a wave of harassment directed at his employer, Dr. Al-Arian found himself politically targeted by the University.

The management of the University of South Florida attempted to dismiss him from teaching and remove him from the campus in spite of his status as a tenured professor on the grounds that the right-wing harassment campaign was compromising campus safety. The move was widely condemned by faculty groups and the American Association of University Professors as a violation of academic freedom.[260] The effort to remove Dr. Al-Arian from the campus was nonetheless supported by Florida state authorities, including Governor Jeb Bush. By 2002, the University authorities had changed their rationale for removing Dr. Al-Arian by alleging that he had supported "terrorism," and that this was a justification for breaching their contract with him.[261]

The federal government's indictment of Dr. Al-Arian on terrorism-related charges in 2003 therefore gave the University legal grounds to finally dismiss him.[262] The charges brought against Dr. Al-Arian and several co-defendants involved financial support for a number of charities that the federal government alleged were fronts for Palestinian Islamic Jihad, an FTO, and allegations that Dr. Al-Arian himself was the leader of the Palestinian Islamic Jihad. The lengthy indictment spelled out a massive conspiracy connecting Dr. Al-Arian's fundraising activities and political views to suicide bombings. The investigation was carried out by the Miami JTTF.[263]

During pre-trial detention, Dr. Al-Arian was kept in solitary confinement. He was placed in ankle and wrist shackles whenever he left his cell, including for his case appointments, being forced to carry his papers on his back. Dr. Al-Arian was also deprived of reading and writing materials, the ability to pray, or to have anything beyond limited contact with his family or attorneys. He was also repeatedly strip-searched while in detention.[264]

At his trial in 2006, the evidence presented by the United States government focused almost entirely on Dr. Al-Arian's political activism for the Palestinian cause, with an emphasis on the statements and speeches he had given. At no point was evidence that his charity work benefitted Palestinian Islamic Jihad provided to jurors. This was in spite of the government having carried out over a decade of surveillance against Dr. Al-Arian.

In a rare loss for the government, the jury acquitted Dr. Al-Arian of eight charges while deadlocking on nine. Dr. Al-Arian was not found guilty of a single charge. To avoid putting himself and his family through greater distress, Dr. Al-Arian attempted to negotiate a plea deal instead of being re-tried on the remaining charges. The government attempted to further criminalize Dr. Al-Arian's activity by calling him to testify in another terrorism-related prosecution; when Dr. Al-Arian refused, believing the defendant in that case was also innocent, he was charged with contempt of court.[265] The government finally dropped most of the remaining charges in 2014, and Dr. Al-Arian was deported to Turkey in 2015 as part of a plea deal.[266]

Several aspects of the Al-Arian prosecution are notable. First, the prosecution brought to light the abusive nature of the alteration of the USA PATRIOT Act to permit FISA investigations to be used for criminal prosecution. Though federal prosecutors alleged that Dr. Al-Arian may have been a foreign agent long before the September 11th attacks, at no point was any effort made to treat him as a perpetrator of a crime on that basis at that time. It was the collapse of the "wall" that permitted putting Dr. Al-Arian behind bars.

Second, despite the broad nature of the statutes utilized by the federal government, the government was unable to build a meaningful case against Dr. Al-Arian that could convince a jury of criminal activity. That the federal government brought charges nonetheless indicates that the government views dissident political views as justification for criminal investigations, including extensive, decades-long surveillance of an

259 - 266 See Appendix

individual's private communications, as well as the communications of his family.

Third, the circumstances of the investigation indicated that the authorities charging Dr. Al-Arian were entirely aware that he posed no threat. The allegations of involvement in "terrorism" extended over a decade, during which Dr. Al-Arian was involved in high-level politics, including a visit to the White House. Nonetheless, both the indictment and his pre-detention portrayed Dr. Al-Arian as an active threat.

Lastly, the prosecution brought out the right-wing and Islamophobic character of the FBI's surveillance campaign. Dr. Al-Arian's prosecution could not be meaningfully removed from the context of his pre-prosecution employment difficulties, which were in turn triggered by a right- wing mob egged on by a talk show host. While few would take the ramblings of a television show host seriously, the collaboration of the university management, who act as representatives of the government of Florida, and the FBI in prosecuting Dr. Al-Arian lent legitimacy to a deeply reactionary narrative.

Targeting Black Muslim Poverty: The Liberty City 7

Another notable prosecution characterized by abusive surveillance practices was the Liberty City 7 case. This prosecution and investigation was led by the Miami JTTF alongside a number of Florida authorities, including the Florida Department of Law Enforcement, the Miami Dade Police Department, the City of Miami Police Department; Broward Sheriff's Office; Palm Beach County's Sheriff's Office; Ft. Lauderdale Police Department; Hollywood Police Department; and the Miramar Police Department.[267]
The investigation targeted several individuals who frequently convened in a rundown warehouse in the Miami neighborhood of Liberty City as members of a religious cult based on the beliefs of the Moorish Science Temple, an African-American offshoot of Islam that fuses Islamic, Christian, and Jewish teachings.

Members of the group followed Narseal Batiste, a former street preacher, to provide community services to people in the local neighborhood. The group mixed a belief system in which Batiste was viewed as a divine leader with genuine efforts to provide services to neighborhood youths. Two paid informants for the FBI who lived nearby suggested that the men might be supporters of Al Qaeda for no apparent reason. In response, the FBI and its partners set up a sting operation in which the informants would offer Batiste and his followers money in exchange for swearing loyalty to Al Qaeda and offering themselves to carry out armed attacks. The nature of the discussed attacks were so far beyond anything that the small group could ever accomplish – including a discussion about blowing up the Sears Tower in Chicago – that the FBI itself appeared to recognize that there was no serious plan to attack anything, calling the plot "more aspirational than operational."[268] Rather, Batiste and the other members maintain that they were simply attempting to trick the faux Al Qaeda agents out of their money. As tensions caused the group to fall apart before the plot went further, government agents arrested the men and charged them with terrorism-related offenses. Despite the significance of the allegations put forward during the arrest – that the men were actually seasoned "terrorists" planning to carry out deadly attacks on Americans – the men were ultimately given short sentences and housed in medium and low security prisons. Two of the seven members were acquitted. All of them have since been released, and two were deported.[269]

Below: Family members of some of the seven men charged with plotting to destroy the Sears Tower in Chicago and other buildings, center left in white t-shirts, look on during a news conference where activists spoke, Thursday, June 29, 2006 at the Liberty City neighborhood warehouse in Miami where the FBI arrested most of the men. (AP Photo/Wilfredo Lee)

The Liberty City 7 prosecution is notable for two reasons. First, the campaign to prosecute the men involved several different coordinating departments. While it is unclear what service was provided by which department, all of the defendants were subject to aggressive surveillance even though the only "Al Qaeda operatives" in question were FBI agents pretending to be Al Qaeda recruiters who initiated contact.

Second, the prosecution indicated that the FBI was willing to go to extreme lengths to target the poor. At no point was there any suggestion that the Liberty City 7 even held the same ideological goals as Al Qaeda. Rather, they were participants of a different faith tradition whose entire record was limited to engaging in community activism without any armed violence. Nonetheless, the authorities expended tremendous resources to surveil, prosecute, jail, and deport the Liberty City defendants.

267 - 269 See Appendix

LOUISIANA

Expansive Surveillance Guidelines at LA-SAFE

Though Louisiana has an aggressive JTTF presence and a state-level fusion center, Louisiana has netted relatively few federal prosecutions since the September 11th attacks. However, it nonetheless serves as an example of how surveillance policies and investigations can intimidate Muslim communities even without extended and public terrorism prosecutions.
Like other fusion centers, the Louisiana State Analytic & Fusion Exchange, or LA-SAFE, is used to gather significant amounts of information without a reasonable suspicion predicate or sufficient protections to avoid discrimination. LA-SAFE also uses the "relevance," "usefulness," and "lawful manner" standards to justify gathering information.[270] With regards to SARs, LA-SAFE explicitly states that information stored by the fusion center need not be based on "reasonable suspicion."[271] While stating that the information cannot be collected based on political or religious affiliations, all prohibitions are qualified with "merely," replicating the problems of the "solely" standard in other information-gathering regulations. A follow-up provision of the policy states that "information is not to be collected on a person because of race, religion, national origin, political affiliation, support of unpopular causes, social views or activities, participation in a particular noncriminal organization or lawful event, citizenship, age, ethnicity, place of origin, disability, gender, or sexual orientation."[272] Because these characteristics are the same as those subject to the "merely" standard, it is unclear exactly what standard LA-SAFE uses when gathering information that implicates these aspects of social life.

Federal-to-Local Spying and the Climate of Fear

The driving force behind anti-Muslim surveillance in Louisiana, as in other states, has been the JTTF. Community members in Louisiana shared stories and documentation going back to the September 11th attacks in which JTTF agents aggressively pressured members of Louisiana mosques to work as informants. Many were questioned without attorneys and were threatened with immigration consequences or other legal issues if they were reticent. Some individuals who have reached out to Project South indicated that they now fear attending mosques and are concerned about government retaliation. Some suspect that they were placed on the government's "no fly list," one of many federal watch-lists used to restrict air travel access, as a result of their refusal to collaborate.

SOUTH CAROLINA

Though Project South could not confirm specific cases of surveillance abuse aimed at Muslims in South Carolina at this time, the policies of the South Carolina Law Enforcement Division and the policies of several South Carolina cities indicate cause for concern.

Expansive Surveillance Guidelines at SCIIC and in Local Police Departments

The South Carolina Law Enforcement Division's South Carolina Information and Intelligence Center (SCIIC) is South Carolina's state-level fusion center. Like the other fusion centers reviewed, SCIIC uses the "relevance," "usefulness," and "fair and lawful" standards for retaining both criminal intelligence information and SARs.[273] It similarly excludes information gathered based on protected characteristics using the problematic "solely" standard.

Notably, the SCIIC policy includes, in an appendix, additional legal analysis about the fusion center's information-gathering and compliance with South Carolina law. The appendix cites State v. Houey, 357 S.C. 106 (2007) for the proposition that the South Carolina constitution provides greater privacy protection than the federal Constitution's Fourth Amendment, but not so much as to prevent the gathering and circulation of information "in a limited way…about individuals for whom a reasonable suspicion of criminal activity exists."[274] While recognizing the dearth of case law, the rule of Houey arguably contradicts the justifications for other forms of information gathering in South Carolina, including the SAR initiative, which plainly does not involve reasonable suspicion.

The Charleston Police Department

The Charleston Police Department's internal policies include language that appears to enable dangerous surveillance practices. First, the Charleston Police Department's Administrative General Order #8 states: "The restriction on the officer's use of race, ethnicity, national origin, religion, age, gender, gender identity/expression, sexual orientation, immigration status, disability, housing status, occupation, or language fluency does not apply to law enforcement activities designed to strengthen the department's relationships with its diverse communities."[275] This language appears to leave room for harmful CVE programs that could function as state surveillance disguised as community outreach. Second, Administrative General Order #37 governing Charleston Police Department's Criminal Intelligence Unit appears to encourage officers to "seek out intelligence through various sources to include but not limited to open source and social media, in attempts to deter or prevent criminal activity that has not yet occurred."[276] This is the language of preventative policing. Information gathered under this policy is shared through a fusion center known as the Seahawk Charleston Interagency Operations Center (SCIOC), which in turn works with the FBI and DHS to identify "pre-incident indicators," which appear to be synonymous with SARs.

---

270 - 276 See Appendix

CHAPTER 5

COMMUNITIES RESIST: SURVEILLANCE.

Despite the intimidation and challenges related to the patterns of surveillance discussed in previous chapters, community groups throughout the country and the U.S. South have not been complacent. Rather, community-led responses have successfully challenged the expansion of surveillance policy and pursued a number of pathways to challenging the surveillance state in various places.

Obstacles and Limits to Traditional Strategies

At the outset, it is worth emphasizing that strategies to challenge surveillance must take into account the unique situation that Muslims in particular and directly-impacted communities in general face with regard to government surveillance practices. Both generalized intelligence-gathering and the use of intelligence gathering for criminal prosecution are domestic extensions of war and structural inequality, building off more than a century of an ingrained and powerful surveillance apparatus with few meaningful legal checks and balances. As such, surveillance programs should not be seen as abstract policy excesses or overzealous reactions to real problems. Rather, they are expressions of the country's deepest racialized inequalities and express some of its most undemocratic tendencies. These policies cannot be meaningfully challenged without building the political power and influence of the communities that are targeted with surveillance.

Compounding this already difficult situation is the reality that much of the Muslim community's organized leadership has not always responded to the threat the community faces in a positive and productive way. Rather, the leadership has sometimes responded by offering itself as an extension of the surveillance state through the embrace of CVE programs, the willingness to operate as informants, or otherwise building collaborative relationships with intelligence agencies. Undoubtedly, some of this response was reluctant, as Muslim community leaders may have been just as intimidated as other community members about spurning those who could jail or deport them. But the consequence of such collaboration has been the collapse of meaningful challenges to the underlying inequalities that Muslims and other impacted communities face from the surveillance state by their leadership. Without strong and coordinated leadership to challenge the surveillance state and the Islamophobia that underpins its manifestations in Muslim communities, intelligence agencies have unsurprisingly been able to portray abusive surveillance efforts as partnerships with Muslim communities rather than threats to the communities' safety, privacy, and liberty.

However, the questionable responses from some in institutional leadership roles within Muslim communities can be contrasted with responses of the wider civil society campaigns against surveillance, many of which are multifaith collaborations and involve challenging different aspects of the surveillance state through various ways. In this chapter, some of these campaigns and their successes are highlighted alongside methods to replicate those successes in the U.S. South.

Before discussing what strategies hold promise, it is worth discussing standard responses to surveillance abuses that are often suggested in community dialogue sessions about surveillance. Specifically, community members often suggest or inquire about countering surveillance abuses through litigation and changes to federal law.

Litigation

Although litigation is an obvious strategy, there are significant costs to pursuing litigation in order to restrict or challenge abusive surveillance practices. The unfriendly legal backdrop summarized in Chapter 3 and the immense costs and lengthy timelines for litigating surveillance abuses mean that it is not often a meaningful source of relief.

The ongoing litigation in Fazaga v. FBI is exemplary of this phenomenon. Though Fazaga was initiated in 2011 after an FBI informant admitted to engaging in surveillance of a California mosque during a separate legal proceeding, the case is still in its procedural phase after nine years. The Ninth Circuit did reverse a state secrets claim by the government to throw out the litigants' claims under FISA, holding that where a claim against the government is made under FISA, that statute and its exemptions govern rather than the state secrets privilege. See Fazaga v. FBI, 916 F.3d 1202 (9th Cir. 2019). However, the FISA framework is not significantly friendlier to litigants and itself poses tremendous barriers for relief.[277]

At first glance, litigation targeting local governments over anti-Muslim surveillance may seem more promising, with litigation aimed at the NYPD over its Muslim Surveillance Program as an example of successful strategic litigation. While no one can deny the success of litigation against the NYPD, certain factors are worth pointing out. First, litigation could only take place after journalists exposed the explosive details and sheer discrimination of the NYPD's spying program to the public. Normally, such details would come out only through discovery, which would require being able to state a legal claim amidst heightened pleading rules that would prevent most lawsuits lacking inside information from going forward. Second, litigants in all three major NYPD lawsuits – Raza, Handschu, and Hassan – had available preexisting guidelines and regulations on NYPD spying that came about through a 1971 settlement agreement that added additional restrictions to the legality of the NYPD's actions. These actions were the straightforward basis of both Raza and Handschu and assisted significantly in a favorable settlement in Hassan.[278] Such a situation does not exist in most places that are engaged in demographic mapping. Finally, the NYPD was subject to considerable political damage as a result of both the leaks and the lawsuit, as its relations with the communities it depended on for policing were strained during an administration that was already under significant criticism for its racial profiling against Black people. Indeed, while the

277 For a detailed analysis of the shortcomings of this litigation victory, see Fazaga v. FBI, Ninth Circuit Holds that FISA Displaces the State Secrets Privilege for Electronic Surveillance, 133 HARV. L. REV. 1774 (2020).
278 Stipulation of the Settlement at 3, Hassan v. City of New York, 804 F.3d 277 (3d Cir. 2015) (discussing the relevance of the Handschu guidelines to the settlement agreement).

"Both generalized intelligence-gathering and the use of intelligence-gathering for criminal prosecution are domestic extensions of war and structural inequality, building off more than a century of an ingrained and powerful surveillance apparatus with few meaningful legal checks and balances."

litigation was successful, an equally important victory in reigning in the NYPD took place not through the courts, but through strong community organizing targeting the city council, which ultimately passed multiple ordinances designed to monitor the NYPD and ban racial and ethnic profiling by the police.[279]

Additionally, federal spying in particular is largely based on an unfriendly legal framework in which the federal government can invoke extensive procedural protections rooted in "national security" as well as enforcing heavy penalties aimed at whistleblowers, and does not face the same level of organized community opposition at the national level. Because much of the known anti-Muslim spying is taking place at the federal level, a litigation-focused model aimed at local governments will rarely bear fruit.

Statutory Changes

Aside from litigation, community members as well as watchdog groups such as the ACLU have called for changes to federal law.[280] While such changes are obviously desirable, the fact remains that the surveillance apparatus is not a broken system in need of fixing. Rather, it is working as federal officials intend with the approval or acquiescence of traditional limits on their actions, such as courts and watchdogs, with minimal oversight, and with the aim of targeting particular political and religious communities.

As such, history tell us that legislative and administrative restrictions on state surveillance only take place in times of significant crisis following leaks of overwhelming abuse, such as the revelations of COINTELPRO, the campaign against CISPES, the Abu Ghraib leaks, and the NSA spying programs leaked by Edward Snowden. Indeed, each of these leaks resulted in some legislative changes, discussed in Chapters 1 and 2.

But each of those reforms were unfortunately mired with significant shortcomings. None of them ultimately restrained the hand of the federal government's spying programs. Lack of transparency, the passage of time following the public's initial outrage, and fearmongering after "terrorist" attacks all resulted in significantly weakening whatever limited reforms the government has been willing to place on its agencies.

But perhaps most importantly, crises that prompted some effort to rein in the federal surveillance apparatus usually involved the perception that the "wrong" people were being spied on. Indeed, while instances like Edward Snowden's leaks of mass data collection sparked at least some outrage among the American public, similar spying scandals involving the federal government that targeted Muslims prompted little outrage outside of Muslim communities and among civil liberties watchdog groups.[281] Polls consistently show that a significant portion of the American public believes that Muslim-Americans deserve to be racially profiled.[282]

But while this situation is discouraging, the fact remains that federal spying initiatives bank heavily on local collaboration for tips, informants, and political legitimacy. All of these aspects of anti-Muslim spying in general have been successfully targeted through local campaigns. The following section discusses several case studies.

Reclaiming Muslim Community Spaces in Atlanta, GA and Kenner, LA

One of the most powerful methods of preventing surveillance abuses against Muslim communities is to organize within existing community spaces to challenge surveillance practices.

During local "Know & Defend Your Rights" workshops, community dialogue sessions, and other local outreach in the Atlanta area, Project South observed that many mosque attendees hold varying views and awareness levels about the seriousness, risk, and drawbacks of government surveillance programs. Like almost all communities within the United States, Muslims in America are often unaware of their own legal rights and the benefits of invoking these rights – an issue compounded by the ambiguities of national security law.

In response, Project South worked to close the knowledge gap on anti-Muslim surveillance and discrimination against Muslims generally by engaging in documentary screenings, speak-out sessions, and "Know & Defend Your Rights" workshops at local mosques and Muslim community and student spaces throughout the Atlanta area, as well as in other parts of the U.S. South. These workshops provide Muslims and other impacted communities spaces to openly discuss and consider the dangers posed by surveillance and brainstorm local solutions to protect their own rights. Project South also provides the free service of limited representation for Muslims and other community members who are contacted for interrogation by law enforcement, including the FBI. In addition to ensuring that Muslims and others know of the dangers posed by the broad legal authority given to federal agents regarding "counter-terrorism," offering limited representation in cases of questioning by law enforcement provides impacted people with the option to direct federal agents to an attorney in the event that they are contacted for questioning. Ensuring that community members both know their right to decline to answer questions and direct agents to an attorney instead is a relatively simple but effective way to limit the threat posed to Muslim communities by intrusive and nerve-wracking visits from federal agents who often take advantage of the vulnerable position of Muslims, particularly immigrant Muslims. This service is a relatively cost-free investment for public interest attorneys that has the

279 - 281 See Appendix

important result of nipping federal intelligence-gathering efforts in the bud.

While visits from government agents at home are an issue, many Muslim communities report the even more disconcerting phenomenon of mosque leadership inviting federal agents and police officers into Muslim spaces to encourage collaboration with federal authorities and to report suspicious behavior. Though there are fewer limits to passive intelligence-gathering efforts by confidential informants in mosques, which are usually open to the public, permission from mosque leadership is required for presentations by government agents. These presentations encourage Muslim community members to actively take part in the surveillance apparatus. Anecdotal reports from Muslim community members who have seen their mosques welcome federal agents suggest that mosque leaders are often themselves fearful of turning away federal agents. However, even informal organizing efforts by mosque attendees to oppose such collaborations have had success.

In Kenner, LA, members of the Abu Bakr Mosque successfully challenged such surveillance collaboration initiatives by using their most important resource: themselves.[283] Mosque leadership, apparently aware that a significant portion of the community was not supportive of any effort at collaboration with the JTTF due to intrusive and threatening experiences with the FBI in the past, avoided publicizing visits from federal agents. Instead, on at least one occasion, the leadership invited federal agents to provide a presentation before a regularly scheduled evening prayer, knowing that attendees would be present. To challenge the presentation, the congregants organized an impromptu walk-out. The significant embarrassment created by a sudden walkout created pressure on the mosque leadership to avoid such presentations in the future. Additionally, the congregants were able to prevent future presentations by challenging the mosque's board of directors through elections.

While not all surveillance of the Muslim community is as visible as home visits or mosque presentations, federal agents do rely on such presentations as a key source of obtaining information. Reclaiming Muslim community spaces through simple efforts such as walk-outs, elections, and other forms of protest can successfully challenge these practices.

Shutting Down CVE Programs in Los Angeles, CA

Throughout the country, CVE programs have come under fire from civil rights organizations and Muslim community groups. Nonetheless, already cash-strapped service organizations are often lured into the CVE process by the offer of grant money. Furthermore, the repeated rebranding of CVE programs, including as "public health" or "community outreach" programs provides a disguise that some groups may find convincing.

But in Los Angeles, Muslim and immigrant community organizers, an anti-surveillance organizing coalition, a large teachers union, and various community organizations managed to carry out a multi-pronged grassroots campaign to force the city council and the mayor to reject a CVE grant from DHS in 2018. Each member of this broad coalition carried out different intersecting roles to ensure the success of their campaign.[284]

First, grassroots organizations like the Palestinian Youth Movement (PYM) and the Stop LAPD Spying Coalition ensured that the community understood what CVE is and the harms it poses by holding weekly information sessions that were open to the public. During these sessions, PYM was able to distribute materials that explained the problems with CVE in multiple languages.[285] In addition to the PYM's mostly Muslim Palestinian community base, the organizations were able to reach community members from various immigrant, refugee, Black, indigenous, Muslim, and Arab communities, including community members who had directly experienced the harmful impacts of surveillance.

The campaign against CVE programs also built on growing opposition to similar "Preventing Violent Extremism" (PVE) grants. Similar in nature to CVE grants, PVE grants come from California state government and also involve a "preventative policing model" that seeks to detect signs of future violence among youth.

As some of the earliest CVE programs had focused on universities, grassroots activists from PYM who had experience working on university campuses with student activists were able to keep track of DHS grant proposals and build links with educators. In addition, the Stop LAPD Spying Coalition had maintained close ties with teachers and youth activists for many years. Building on their relationships with educators, the grassroots activists were able to approach leaders in the United Teachers Los Angeles, a 30,000-member teachers' union to explain the issue and the dangers posed by CVE and PVE programs, noting that PVE programs carried out in other cities essentially incentivized teachers to criminalize their own students. According to activists from PYM and Stop LAPD Spying, this history made opposition to PVE and CVE among UTLA an easy sell.[286] Indeed, only two years before, the American Federation of Teachers had issued its own strong statement expressing outrage over the use of similar programs that the FBI and DOJ had advocated.[287] In a letter to Los Angeles authorities, the UTLA expressed the position its House of Representatives had adopted, strongly opposing CVE and PVE grants.[288]

---

282 - 288 See Appendix

At the same time, coalition member groups, with the support of educators and youth activists, ensured that the public repeatedly flooded the LA City Council whenever the CVE grant was on the agenda. This process ensured that the city council knew that the issue was not an abstract political matter that was mobilizing a small number of people; rather, it sparked opposition among key and sizeable constituent groups that were active and mobilized and considered stopping the CVE grant a significant issue. PYM and Stop LAPD Spying helped mobilize educators and youth activists from various communities to attend these direct actions at City Hall to make public comment.

Finally, attorneys from CAIR, Asian-Americans Advancing Justice, and the ACLU filed state and federal records requests about the program and a lawsuit against DHS for failing to turn over the proper records.[289] Emphasizing the lack of information and transparency behind the CVE grant itself, organizers were able to accurately portray the CVE program not as a humanitarian effort to provide aid, but rather as an opaque effort by DHS to use local governments to spy on targeted communities. By demanding more information about the CVE program, DHS and the LAPD could not hide behind attempts to rebrand the program without contradicting any disclosures they were required to make. Ultimately, the failure to provide proper disclosures – such as what criteria would be used to determine if someone was being "radicalized" – prompted litigation. Failure by both DHS and city authorities to disclose such vital information about the grant made it difficult to defend the grant's purpose. As such, while litigation took place, its practical function was to lend greater credibility to the grassroots political campaign.
Ultimately, community opposition prompted enough delay in the process that the mayor of LA rejected the CVE grant.[290] Organizers of the campaign have since set their focus on California's state-level PVE grant program. Similar success stories in shutting down CVE grants have emerged out of Chicago, Boston, and Minneapolis.

Ending JTTF Agreements in San Francisco, CA

As discussed in Chapter 2, FBI JTTF arrangements are one of the primary ways through which the FBI has been able to mobilize local policing resources in different states to surveil and entrap Muslims using overbroad "counter-terrorism" legislation. Amid community pressure, several cities have ended JTTF agreements with the FBI over criticism of the FBI's lack of respect for local restrictions on policing. One remarkable campaign to end the arrangement took place in San Francisco.

The San Francisco Police Department (SFPD) entered into a Memorandum of Understanding with the FBI in 2002.[291] While this original MOU included a number of requirements ensuring that any SFPD involvement would be subject to local policy restrictions on discrimination and surveillance, those requirements were discarded in 2007 in secret.[292]

Notably, this included SFPD's compliance with General Order 8.10, adopted in 1990, which required reasonable suspicion to investigate criminal activity and placed restrictions on the authority of SFPD officers to investigate political and religious activity.[293] The order was expanded in the aftermath of a spying scandal in which the Anti-Defamation League, a Jewish organization that doubles as a pro-Israel lobbying organization, collaborated with a former SFPD detective to spy on civil rights organizations over suspected sympathy among their members toward the Palestinian plight. The order was amended to require audits to monitor compliance with the order.[294]

But the secret 2007 MOU between the SFPD and the JTTF removed this restriction, and instead subjected SFPD officers working with the JTTF to only the restrictions required of federal agents. As discussed above in Chapter 2, these restrictions, embodied at the time in the Mukasey guidelines, were extremely permissive.

Amidst reports of aggressive FBI intelligence-gathering in the San Francisco Bay Area, often under the guise of community outreach, civil rights groups filed FOIA requests and one lawsuit to turn over information about the scope of FBI intelligence-gathering.[295] The FBI's conduct prompted the creation of the Coalition for a Safe San Francisco, which in turn managed to obtain the text of the 2007 Memorandum of Understanding through a records request.

These revelations prompted the Coalition, led by Arab-American organizers such as the Arab Resource and Organizing Center (AROC), to create a community-led pressure campaign against the San Francisco municipal government to reign in the FBI. In late 2010, the San Francisco Human Rights Commission held a detailed hearing on the concerns of the community, led by a variety of groups involved in the Coalition. The hearing culminated in a report on the dangers of surveillance and the erosion of civil liberties protections, and a series of recommendations to San Francisco's Board of Supervisors, which functions as the city council.[296] With the community actively engaging the existing institutions of local government, the Coalition worked with Supervisor Jane Kim, who introduced an ordinance that would prohibit SFPD officers from working with the JTTF without following the SFPD's internal guidelines.[297] Amid mass protests organized by the Coalition, testimony from affected community members in front of the Public Safety Commission, and a phone campaign to pressure Supervisors to vote for the bill, the Coalition was able to secure six of the eleven votes in favor of the legislation.[298]

---

289 - 298 See Appendix

Unfortunately, this was insufficient to override a mayoral veto. But rather than giving up, the Coalition then lobbied the mayor himself, who ultimately accepted a weakened version of the bill that was passed unanimously.[299]

Under the ordinance, all SFPD officers must abide by local and state regulations rather than federal ones, any changes to the memorandum of understanding must be submitted to the Police Commission for public comment and discussion, and a public report on compliance with the ordinance must be provided each year.[300] Missing from the weakened ordinance were additional, specific restrictions on SFPD involvement in particular types of FBI investigations.

Below: A local professor speaks out at a rally to restrict the MOU (AROC).

In ensuing years, however, it became clear that the SFPD and FBI were not properly disclosing all relevant information and Muslim community members continued to face police harassment. Having won the battle to pass the ordinance, community groups went on to enforce it by filing municipal complaints against officers whom they believed were violating the terms of the ordinance and demanding further information from the city when it became clear that public disclosures were not including all instances in which Muslims were being harassed by federal or SFPD agents.[301] Post-hoc disclosures suggest that during this time, the SFPD and FBI were aware of the significant contradictions between what SFPD officers were authorized to do and what JTTF expected them to do. Despite publicly claiming that all SFPD activities with JTTF abided by local laws, these disclosures indicated that the FBI was in fact having SFPD officers carry out "assessment" investigations that intruded on First Amendment-protected activity in apparent violation of the ordinance.[302]

Amidst increasing scrutiny and the demand for more compliance and information from grassroots advocates and civil rights groups, as well as the inauguration of an openly Islamophobic president, the SFPD suddenly announced its withdrawal from the JTTF MOU in early 2017.[303] While there is some discussion of the SFPD returning to work with the JTTF, the record that the SFPD left behind indicates that the program is fraught with legal contradictions and earned the opposition of the public.

The experience of advocates in San Francisco reveal a number of lessons. First, the JTTF is not transparent about its activities and will deceptively conceal them from the public. This was true both before the passage of the resolution, when the JTTF and local police changed the memorandum of understanding without the public's knowledge, and after, when the agencies improperly withheld information indicating violation of the ordinance. Second, it indicates that local ordinances, when enforced vigorously through community advocacy, complaints, and demands for transparency, can create the necessary political tension between departments which are required to accept stringent constitutional limits and federal agents who are not. Lastly, it signifies that grassroots advocacy campaigns that might be insufficient to trigger change at the federal level – such as phoning members of the government, holding protests, or testifying in front of committees – may be sufficient for passing local legislation that would force the hand of the FBI to recognize stringent legal limits or risk losing local collaboration. Coalition groups counted a second victory in October 2020 when the Oakland Police Department also announced its withdrawal from the JTTF under community pressure following a similar campaign.[304]

Halting the Expansion of Fusion Centers in Georgia

The Georgia Information Sharing and Analysis Center (GISAC), a fusion center discussed in Chapter 3, was created in October 2001 to coordinate "counter-terrorism" surveillance efforts. In practice, there is no terrorism-related limit to its function and it exists to detect "threats" of all kinds.

A coalition of immigrants' rights activists took notice when a Georgia state law, Senate Bill 15, suggested expanding the role of GISAC into monitoring Georgia schoolchildren.[305] Proposed by Republican lawmakers in the aftermath of a school shooting, SB15 would have required GISAC to create individualized profiles of students to evaluate potential threats posed by them, and share this information with the Georgia Emergency Management and Homeland Security Agency (GEMA-HS). In addition, the bill required GEMA-HS to train individuals selected from among former military and police officers to function as "school safety coaches."

Concerns over the bill were numerous.[306] In addition to the threat that GISAC posed to Muslim communities in particular, campaigners noted that the bill would place undocumented immigrant students in a position of considerable vulnerability

299 - 306 See Appendix

if information related to their immigration status was gathered and turned over to Georgia authorities. Furthermore, existing studies suggested that students of color are already likely to face greater disciplinary action in schools, and the use of police and military in place of traditional school authorities would exacerbate the risk of violent abuse of students.

As such, Project South worked with a coalition of dozens of groups, including the Georgia Latino Alliance for Human Rights, Black Alliance for Just Immigration, and Women Watch Afrika, to challenge the bill. Amid opposition expressed by community activists who took to the Georgia State Capitol to lobby representatives and testify against the bill, the bill was amended to exclude the school safety commissioner and student profile provisions.[307]

Nonetheless, the amended version of the bill still required school officials to turn over a broad array of information to GISAC.[308] The amended bill passed through the Georgia legislature with a majority of Georgia senators supporting it, to be signed into law by Governor Brian Kemp.

Mobilizing the same grassroots coalition to deliver hundreds of signatures to the Governor, Project South coordinated a last-ditch effort to prevent the bill from being signed into law. The Governor ultimately vetoed the bill, stating that local governments already had the necessary resources to keep students safe.

This victory is notable for several reasons. First, although the legislative climate was not friendly, the grassroots coalition was able to significantly weaken the bill even before it passed, and the governor vetoed the bill despite its passage through the legislature.

Indeed, early reports suggested that generalized concerns about privacy prompted some outcry among more conservative citizens groups as well

The concerns that the coalition raised were privacy issues not limited to any particular constituency. As such, the campaign proved that even lobbying governments dominated by conservatives can occasionally produce positive results, and that grassroots activists should not be demoralized when engaging in local organizing against surveillance due to the political climate.

Second, the coalition was diverse and led by immigrants' rights groups without a Muslim-majority base. The anti-SB15 campaign is a model for how Muslim community organizing campaigns can bridge the gap between Muslims and other constituencies.

Above: Coalition members deliver hundreds of signatures to the Governor's Office demanding he veto SB 15. (Project South)

307 Ty Tagami, Georgia Legislature passes school security bill, ATLANTA JOURNAL-CONSTITUTION (Apr. 3, 2019).
308 Id. Project South continued to express concern. See Project South, SB 15 Threatens the Safety of Georgia's Students of Color (Updated), available at https://projectsouth.org/wp-content/uploads/2019/04/4.14-SB-15-Final-Updated-Fact-Sheet.pdf?fbclid=IwAR2nITVI4gxdHwBUeGVWFs0cVKDA4i4lDmRtZmlQ_et2ig312dsGxqgEOKc.

"As demands for reigning in abusive, discriminatory, and lethal policing practices capture the hearts and minds of millions of people, it is imperative that social movements demand an end to the mass surveillance of society generally and against directly-impacted communities in particular."

CONCLUSION AND RECOMMENDATIONS

At the time of the publication of this report, a massive organizing effort towards police defunding and abolition has gripped the United States. While these significant changes have been placed on the agenda after being long derided as extreme demands, the same government agencies being scrutinized are engaging in abuses of authority that millions of Americans have begun protesting. In the process, the government has explicitly utilized its "counter-terrorism" authorities to coordinate repression of the demonstrations, as discussed in Chapter 2.

As demands for reigning in abusive, discriminatory, and lethal policing practices capture the hearts and minds of millions of people, it is imperative that social movements demand an end to the mass surveillance of society generally and against directly-impacted communities in particular.

While this report seeks to explain the history, law, and governmental practices behind surveillance and the various forms of resistance against it, the future remains unwritten. For those reasons, Project South offers readers from Muslim, Black, and immigrant communities the following recommendations:

- Apply lessons from the success stories documented in Chapter 5 through community organizing on a local level. Through organized action, our communities protect our families and shield ourselves from surveillance abuses. Members of an active and mobilized community that defends their rights from surveillance abuses are far safer than members of a community who are easily intimidated into sharing sensitive information, particularly where the information sought is increasingly untethered from actual wrongdoing.
- Embrace privacy-oriented technology. Communities should investigate and switch their communications away from data-hoarding and unsecure technologies that collaborate closely with government agencies, such as Google or Facebook, and communicate using channels that permit end-to-end encryption and anonymity, such as Signal and Tor.
- Never speak to police or intelligence agents without an attorney present. Project South and many community groups hold know-your-rights trainings to advise individuals on their rights when approached by officers. Individuals should have an action plan in place in the event of such an encounter, including a statement refusing to answer any questions and asking the officer to leave their contact information. Community members should be advised to contact an attorney to provide limited legal representation for the purpose of addressing questions immediately after being approached. Project South provides this service for free.

Project South hopes this report can be a resource to communities across the U.S. South as we confront surveillance abuses.

Amith Gupta, Esq. prepared this report as part of his 2019 Fellowship with Project South. Project South is a 35 year-old grassroots movement building organization rooted in the Black Radical Tradition. Amith Gupta is an attorney from the Bay Area of California. He holds a Juris Doctor from the New York University School of Law, where he was an Institute for International Law and Justice Scholar, and a Bachelor of Arts degree from Bard College, where he studied Political Studies and Middle Eastern Studies.

The author would like to thank the entire Project South team for providing resources, support, and funding for this project. In particular, the author wishes to thank Azadeh Shahshahani, Manzoor Cheema, Priyanka Bhatt, and Nathan Hunter for their insight and contributions.

1 Andrew Lawler, Muslims Were Banned From the Americas as Early as the 16th Century, SMITHSONIAN, February 7, 2017, https://www.smithsonianmag.com/history/muslims-were-banned-americas-early-16th-century-180962059/.

2 Deepa Kumar, ISLAMOPHOBIA AND THE POLITICS OF EMPIRE, Ch. 2 (2012).

3 Edward E. Curtis, The Black Muslim Scare of the Twentieth Century, ISLAMOPHOBIA IN AMERICA 75, 78-84.

4 William Costel Tamplin, Who Was 'Umar ibn Sayyid? A Critical Reevaluation of the Translations and Interpretations of the Life, J. ARABIC AND ISLAMIC STUDIES 125 (2016); Safet Dabovic, Out of Place: The Travels of Nicholas Said, CRITICISM 59 (2012).

5 Id.

6 Mariam Elba, How Islamophobia was Ingrained in America's Legal System Long Before the War on Terror, THE INTERCEPT (May 6, 2018); Khaled Beydoun, 'Muslim Bans and the (Re)Making of Political Islamophobia, 2017.5 ILL. L. R. 1734 (2017).

7 Curtis, supra note 3 at 84.

8 Kumar, supra note 2 at Ch. 7.

9 Office of the Inspector General of the U.S. Department of Justice, The September 11 Detainees: A Review of the Treatment of Aliens held on Immigration Charges in Connection with the Investigation of the September 11 Attacks (2003).

10 Arun Kundnani & Deepa Kumar, Race, surveillance, and empire, INT'L SOCIALIST REV. 96:3 (2015).

11 Id. at 4.

12 Ward Churchill, From the Pinkertons to the PATRIOT Act: The Trajectory of Political Policing in the United States, 1870 to the Present, 4 CR: THE NEW CENTENNIAL REVIEW 1, 3 (2004).

13 Id. at 16-17.

14 Alfred W. McCoy, POLICING AMERICAS EMPIRE: THE UNITED STATES, THE PHILIPPINES, AND THE RISE OF THE SURVEILLANCE STATE, 293 (2011).

15 Id. at 295.

16 It may be worth emphasizing that just as in the contemporary period, the rise of federal political policing also came alongside the establishment of political police at the state and municipal level, such as "Red Squads." For example, the NYPD created specialized units to target "Anarchists" and political causes associated with Eastern European immigrants as early as the turn of the twentieth century. See Frank Donner, PROTECTORS OF PRIVILEGE: RED SQUADS AND POLICE REPRESSION IN URBAN AMERICA (1992).

17 William H. Thomas, UNSAFE FOR DEMOCRACY: WORLD WAR I AND THE U.S. JUSTICE DEPARTMENT'S COVERT CAMPAIGN TO SUPPRESS DISSENT, 10 (2008).

18 Id. at 3.

19 Id. at 31.

20 Tim Weiner, ENEMIES: THE HISTORY OF THE FBI, CH. 5 (2012).

21 Id. at ch. 6.

22 Id.

23 Adam Hochschild, When America Tried to Deport its Radicals, THE NEW YORKER (Nov. 11, 2019).

24 The FBI's Fraught, Complex History with Black America, DETROIT TODAY (Feb. 8, 2018) https://wdet.org/posts/2018/02/08/86382-the-fbis-fraught-complex-history-with-black-america/./

25 Olmstead v. United States, 277 U.S. 438 (1928) (holding that without a physical trespass, the police do not violate the Fourth Amendment when collecting private communications, such as by wiretapping phone conversations).

26 Curtis, supra note 3 at 90.

27 John Pike, Federal Bureau of Investigation – History, FEDERATION OF AMERICAN SCIENTISTS (2003), available at https://fas.org/irp/agency/doj/fbi/fbi_hist.htm.

28 Id.

29 Curtis, supra note 3 at 91-92.

30 Staff of the S. Select Comm. to Study Governmental Operations with respect to Intelligence Activities, 94th Cong., Report on Intelligence Activities and the Rights of Americans, Book 2, 5.

31 Id. at 6-7.

32 Id. at Book 3, 800-804.

33 Id.

34 Id. at Book 3, 223.

35 Id. at Book 3, 188.

36 Id. at Book 3, 491-492.

37 Id. at Book 2, 11.

38 Id. at 179.

39 Id. at 177.

40 Id. at 10.

41 Id. at 9.

42 Id. at Book 3, 251, 361

43 Id. at Book 2, 7.

44 Id. at 63, 244; Book 3, 452-454.

45 David Cole & James X. Dempsey, TERRORISM AND THE CONSTITUTION: SACRIFICING CIVIL LIBERTIES IN THE NAME OF NATIONAL SECURITY, 85-86 (2006).

46 Office of the Inspector General of the U.S. Department of Justice, The Federal Bureau of Investigation's Compliance with the Attorney General's Investigative Guidelines (2005).

47 Id.

48 Electronic Frontier Foundation, History of FOIA, https://www.eff.org/issues/transparency/history-of-foia.

49 For a discussion on the creation of FISA and its evolution, see Elizabeth Gotein and Faiza Patel, What Went Wrong with the FISA Court, BRENNAN CENTER 9 (2015).

50 For an analysis of the abuses by the CIA specifically, see Comm. On CIA Activities Within the United States, Report to the President 9-42 (1975) (A Report documenting many of the same surveillance abuses also discussed by the Church Committee Report); and Select Comm. On Intelligence and the Subcomm. On Health and Scientific Research of the Comm. On Human Resources, United States Senate, 95th Cong., Project MKULTRA, The CIA's Program of Research in Behavioral Modification (Aug. 3, 1977) (A Senate Committee Report extensively discussing the MKULTRA Program); Terry Gross, The CIA's Secret Quest for Mind Control: Torture, LSD and a "Poisoner in Chief ", NPR (Sept. 9, 2019) (discussing the MK-ULTRA Program, a program carried out by the CIA from 1953 to 1964 in which the CIA abused and drugged numerous test subjects in a quixotic effort to achieve mind control).

51 Exec. Order No. 12,333, United States Intelligence Activities, available at https://dodsioo.defense.gov/Library/EO-12333/.

52 Office of the Inspector General, supra note 46; Cole & Dempsey, supra note 45 at 85.

53 Office of the Inspector General, supra note 46. ABSCAM was an FBI sting operation focusing on public corruption aimed at multiple government institutions, including the United States Senate. Operation Corkscrew was a probe against case-fixing in the Cleveland Municipal Court that involved undercover investigators but produced no useful evidence for prosecution.

54 Id.

55 Id.

56 Cole & Dempsey, supra note 45 at 41.

57 Office of the Inspector General, supra note 46.

58 Cole & Dempsey, supra note 45 at 102.

59 See Sherri J. Conrad, Executive Order 12,333: Unleashing the CIA Violates the Leash Law, 70 CORNELL L. R. 968, 972-976 (1985).

60 Id, generally.

61 While it partially precedes the FTO list, the deference to Executive Branch officials on determining who is a "terrorist" has led to some embarrassing contradictions. For example, in 2012, after aggressive lobbying from its supporters, the Secretary of State removed the Mujahideen e-Khalq (MEK) from the list despite its well-established history of bombings and violent activity. Likewise, pre-AEDPA designations resulted in placing Nelson Mandela, the leader of the anti-Apartheid movement in South Africa, on a list of designated "terrorists" until he was removed from the list by an act of Congress in 2008.

62 Reno v. American-Arab Anti-Discrimination Comm., 525 U.S. 471 (1999).

63 Open Society Justice Initiative, Globalizing Torture: CIA Secret Detention and Extraordinary Rendition, 13-14 (2013).

64 Id.

65 President's Address Before a Joint Session of the Congress on the United States Response to the Terrorist Attacks of September 11, in 37 WEEKLY COMP. PRES. DOC. 1347, 1347-49 (Sept. 20, 2001).

66 For a discussion on the Bush Administration's legal justifications for its "war" on terrorism and their absurdity, see Mary Ellen O'Connell, The Legal Case against the Global War on Terror, 36 CASE W. RES. J. INT'L L. 349 (2004). See also Int'l Cmte of the Red Cross, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, 32IC/15/11 (Dec. 8-10, 2015) ("As repeatedly asserted, the ICRC considers that, from a legal perspective, there is no such thing as a "war against terrorism." With respect to the various armed conflicts and the numerous counter-terrorism measures at the domestic and international levels…the fight against terrorism involves, apart from the use of force in certain instances, the use of other measures, such as intelligence gathering, financial sanctions and judicial cooperation"); and Bruce Ackerman, The Emergency Constitution, 113 Yale L.J. 1029, 1032-133 (2004) ("…anybody can be suspected of complicity with al Qaeda. This means that all of us are, in principle, subject to executive detention once we treat the 'war on terrorism' as if it were the legal equivalent of the war against [a country]. War between sovereign states also comes to an end…but this will not happen in the war against terrorism…If the President is allowed to punish, as well as to detain, the logic of war-talk leads to the creation of a full-blown alternative system of criminal justice for terrorism suspects").

67 Aziz Z. Huq and Christopher Muller, The War on Crime as Precursor to the War on Terror, 36 Int'l J. L. Crime & Justice 215-229 (2008).

68 Bush: U.S. at war with 'Islamic fascists'. CNN (Aug. 10, 2006) available at https://www.cnn.com/2006/POLITICS/08/10/washington.terror.plot/.

69 The events of this detention are covered in Office of the Inspector General, supra note 9.

70 Center for Human Rights and Global Justice, Asian American Legal Defense and Education Fund, Under the Radar: Muslims Deported, Detained, and Denied on Unsubstantiated Terrorism Allegations, NYU SCHOOL OF LAW (2011). The NSEERS program was suspended in 2011, though its logic continued to pervade immigration policy and would soon be replaced by more extreme policies under the Trump Administration, discussed infra.

71 Amna Akbar, Policing "Radicalization", 3 U.C. IRVINE L. REV. 809, 812 (2013); Jon Sherman, "A Person Otherwise Innocent": Policing Entrapment in Preventative, Undercover Counterterrorism Investigations, 11 J. CONST. L. 1475.

72 Sherman, Id. at 1475-1478.

73 Akbar, supra note 71 at 811.

74 Id. at 827.

75 Faiza Patel and Meghan Koushik, Countering Violent Extremism, BRENNAN CENTER 9 (2017), available at https://www.brennancenter.org/sites/default/files/publications/Brennan%20Center%20CVE%20Report_0.pdf.

76 Id.

77 Cora Currier, How Community Outreach Programs to Muslims Blur Lines Between Outreach and Intelligence, THE INTERCEPT (Jan. 21, 2015).

78 Alex Ruppenthal and Asraa Mustafa, As Trump relaunches Countering Violent Extremism, records on past Illinois program reveal links to FBI, law enforcement. THE CHICAGO REPORTER, Aug. 14, 2020.

79 Office of the Inspector General of the U.S. Department of Justice, A Review of the FBI's Investigations of Certain Do-mestic Advocacy Groups (September 2010).

80 Federal Bureau of Investigation, Domestic Investigations and Operations Guide, 32 (2008).

81 U.S. Department of Justice, Guidance Regarding The Use Of Race By Federal Law Enforcement Agencies (2003). See also, Carlos Torres, Azadeh Shahshahani, & Tye Tavaras, Indiscriminate Power: Racial Profiling & Surveillance Since 9/11, 18 U. PA. J. L. & SOC. CHANGE 283, 296 (2015).

82 ACLU, EYE on the FBI: The FBI Is Engaged In Unconstitutional Racial Profiling and Racial "Mapping" (2011).

83 Center for Human Rights and Global Justice, Targeted and Entrapped: Manufacturing the "Homegrown Threat" in the United States (2011), 33.

84 Id. at 26.

85 For an extensive report on the use of informants in such prosecutions, see Coalition for Civil Freedoms, Inventing Terrorists: The Lawfare of Preemptive Prosecution (2019).

86 Factsheet: The NYPD Muslim Surveillance Program, ACLU, available at https://www.aclu.org/other/factsheet-nypd-muslim-surveillance-program.

87 Handschu v. Special Services. Div., 605 F. Supp. 1384 (S.D.N.Y 1985); Handschu v. Police Dep't, 241 F. Supp. 3d 433, 438 (S.D.N.Y. 2017).

88 The entirety of this section relies on the information uncovered and documented in S. Comm. On Armed Services, 110th Cong., Rep. on Inquiry Into the Treatment of Detainees in U.S. Custody (2008) (hereinafter "Senate Armed Services Committee Torture Report"), and Select S. Comm. On Intelligence, 113th Cong, Rep. of the Central Intelligence Agency's Detention and Interrogation Program (2014) (hereinafter "Senate Intelligence Committee Torture Report"). For a collection of relevant internal policy documents discussing both the process of legalizing torture and approving specific tactics, including correspondence between OLC lawyers indicating that the legal interpretation they selected was designed to avoid criminal prosecution for torture, see Mark Danner, TORTURE AND TRUTH: AMERICA, ABU GHRAIB AND THE WAR ON TERROR (2004) at Appendix I.

89 Senate Intelligence Committee Torture Report, Id. at 11.

90 Id. at 12.

91 For a summary of the evolution of this litigation, see Steve Vladeck, The Supreme Court Goes to War: Hamdi, Padilla, and Rasul at 10, JUST SECURITY (June 27, 2014), available at https://www.justsecurity.org/12260/supreme-court-war/.

92 Dana Priest, CIA Holds Terror Suspects in Secret Prisons, WASHINGTON POST (Nov. 2, 2005).

93 Bush acknowledges secret CIA prisons, ASSOCIATED PRESS (Sept. 6, 2006).

94 Dana Priest, Wrongful Imprisonment: Anatomy of a CIA Mistake, Washington Post (Dec. 4, 2005) (discussing CIA errors and citing a CIA Inspector General report that the CIA had made numerous renditions of the wrong people).

95 Senate Intelligence Committee Torture Report, supra note 88; Dana Priest, Id.

96 Senate Intelligence Committee Torture Report, Id. All of the incidents and details described in this paragraph are derived from this report.

97 Open Society Justice Initiative, supra note 62 at 15; see also Jane Mayer, Outsourcing Torture: The Secret History of America's "Extraordinary Renditions" Program, THE NEW YORKER (Feb. 14, 2005).

98 Id. See also, Priest, supra note 94.

99 Id.

100 For background information on Mr. Arar's case, see The Rendition Project, Maher Arar available at https://www.therenditionproject.org.uk/prisoners/arar.html.

101 Id.

102 Senate Armed Services Committee Torture Report, supra note 88.

103 Office of the Prosecutor, International Criminal Court, Report on Preliminary Examination Activities (2016), 47-50.

104 Senate Armed Services Committee Torture Report, supra note 88.

105 Id. at xxiv.

106 Danner, supra note 88 at 15, 30.

107 Id. at 3, 31.

108 Id. at 43.

109 Information on what happened at Abu Ghraib is most extensively covered in U.S. Army, Article 15-6 Investigation of the 800th Military Police Brigade (2004) ("The Taguba Report"); Human Rights Watch, The Road to Abu Ghraib, (June 8, 2004); and Danner, supra note 88 at 10 ("The Logic of Torture"). All incidents discussed int his paragraph are described in depth in these reports.

110 Daniel Tencer, Journalist: Women raped at Abu Ghraib were later 'honor killed,' RAW STORY (Sept. 11, 2010), available at https://www.rawstory.com/2010/09/women-abu-ghraib-honor-killed/.

111 Geraldine Sealey, Hersh: Children Sodomized at Abu Ghraib, on tape, SALON (July 14, 2004) ("Some of the worst things that happened you don't know about, okay? Videos, um, there are women there. Some of you may have read that they were passing letters out, communications out to their men. This is at Abu Ghraib ... The women were passing messages out saying 'Please come and kill me, because of what's happened' and basically what happened is that those women who were arrested with young boys, children in cases that have been recorded. The boys were sodomized with the cameras rolling. And the worst above all of that is the soundtrack of the boys shrieking that your government has. They are in total terror. It's going to come out"); available at https://www.salon.com/test2/2004/07/15/hersh_7/.

112 Soldiers convicted in Abu Ghraib scandal, ASSOCIATED PRESS (Oct. 16, 2006).

113 Amnesty International, Beyond Abu Ghraib: Detention and Torture in Iraq, (March 2006), available at https://www.amnesty.org/download/Documents/76000/mde140012006en.pdf.

114 See, e.g. Office of the Press Secretary, President's Statement on Signing of H.R. 2863, the "Department of Defense, Emergency Supplemental Appropriations to Address Hurricanes in the Gulf of Mexico, and Pandemic Influenza Act, 2006," (Dec. 30, 2005).

115 Exec. Order No. 13491, Ensuring Lawful Interrogations.

116 Exec. Order. No. 13493, Review of Detention Policy Options.

117 Department of Justice Office of Public Affairs, Special Task Force on Interrogations and Transfer Policies Issues Its Recommendations to the President (Aug. 24, 2009).

118 Beth Van Schaack, The Torture Convention & Appendix M of the Army Field Manual on Interrogations, JUST SECURITY (Dec. 5, 2014), available at https://www.justsecurity.org/18043/torture-convention-appendix-army-field-manual-interrogations/.

119 Louis Jacobson, Extraordinary Rendition Officially Ruled Out, But Secrecy Makes its Elimination Hard to Prove, POLITIFACT (Dec. 4, 2012).

120 Kenneth Roth, Obama & Counterterror: the Ignored Record, HUMAN RIGHTS WATCH (Feb. 5, 2015), available at https://www.hrw.org/news/2015/02/05/obama-counterterror-ignored-record. See also "The State Secrets Hurdle," chapter two infra.

121 George Brown, Notes on Terrorism Trial, 4 HARV. NAT'L SEC. J. 1, 25 (2012) discusses the way in which prosecutors have sought to portray a "global jihad movement" as a single international conspiracy toward which one can be accused of providing material support under 2339A.

122 Robert M. Chesney, Beyond Conspiracy? Anticipatory Prosecution and the Challenge of Unaffiliated Terrorism, 80 S. CAL. L. REV. 425, 474 (2007).

123 Brown, supra note 121.

124 Id.

125 Id.

126 Nancy Hollander, The Holy Land Foundation Case: The Collapse of American Justice, 20 WASH. & LEE J. CIV. RTS. & SOC. JUST. 45 (2013).

127 d. For a comprehensive look at the impact of material support prosecutions on charitable contributions, see ACLU, Blocking Faith, Freezing Charity: Chilling Muslim Charitable Giving in the "War on Terrorism Financing" (2009).

128 Office of the Inspector General of the Department of Defense, Department of Justice, Central Intelligence Agency, National Security Agency, Office of the Director of National Intelligence, Unclassified Report on the President's Surveillance Program, 4 (2009).

129 Telephony metadata is technical information related to a phone call, such as to what number a call was made, its duration, and other information excluding the actual contents of a phone conversation.

130 James Risen and Eric Lichtblau, Bush Lets U.S. Spy on Callers Without Courts, NEW YORK TIMES (Dec. 16, 2005); Id.

131 Office of the Inspector General, supra note 128 at 11.

132 James Risen and Eric Lichtblau, Spy Agency Mined Vast Data Trove, Officials Report, NEW YORK TIMES (Dec. 24, 2005); Leslie Cauley, NSA Has Massive Database of Americans' Phone Calls, USA TODAY (May 11, 2006).

133 Gotein and Patel, supra note 49 at 21.

134 Id. at 22; Glenn Greenwald, NSA Collecting Phone Records of Millions of Verizon Customers Daily, GUARDIAN (June 6, 2013).

135 Office of the Inspector General of the U.S. Department of Justice, A Review of the Federal Bureau of Investigation's Use of National Security Letters, (March 2007) at 40.

136 Charles Doyle, National Security Letters in Foreign Intelligence Investigations: A Glimpse at the Legal Background, CONGRESSIONAL RESEARCH SERVICE (July 31, 2015).

137 See, e.g. U.S. v. Rosen, 447 F.Supp 2d 538 (E.D. Va. 2006) for a discussion about how courts, like federal agencies themselves, have used First Amendment protected activity to designate someone as a foreign agent.

138 George Zornick, Remember When NSA Surveillance Was Used to Help Launch the Iraq War?, THE NATION (June 11, 2013) (discussing leaked NSA memos detailing the surveillance of undecided U.N. delegations in the lead up to the U.S. invasion). See also, Snowden Archive, The UN Security Council: (SIGINT) History Repeats Itself!, THE INTERCEPT (Aug. 10, 2016), available at https://www.thenation.com/article/archive/remember-when-nsa-surveillance-was-used-help-launch-iraq-war/.

139 These practices are summarized in newsletter-style messages sent by NSA director Michael Hayden to NSA employees, known as "WARgrams" in the aftermath of the invasion. For a summary of the WARgrams, see Jason Koebler, New Docs Show How the NSA Used the Iraq War to Build its Surveillance Apparatus, VICE (Sept. 6, 2016), available at https://www.vice.com/en/article/bmvyd5/nsa-wargrams-show-how-nsa-built-surveillance-apparatus . See also, Snowden Archive, Dispatch from NIST Baghdad: Life in the Palace, THE INTERCEPT (Aug. 10, 2016) (a leaked document discussing the NSA's involvement in attempting to hunt down individuals that the U.S. considered high-value insurgent targets in Iraq).

140 Micah Lee, Margot Williams and Talya Cooper, Sloppy U.S. Spies Misused a Covert Network For Personal Shopping – And Other Stories from Internal NSA Documents, THE INTERCEPT (Sept. 13, 2007), available at https://theintercept.com/2017/09/13/sloppy-u-s-spies-misused-covert-network-for-personal-shopping-and-other-stories-from-internal-nsa-documents/; Micah Lee, NSA Cracked Open Encrypted Networks of Russian Airlines, Al Jazeera, and Other "High Potential" Targets, THE INTERCEPT (Aug. 15, 2018), available at https://theintercept.com/2018/08/15/nsa-vpn-hack-al-jazeera-sidtoday/.

141 Cora Currier, NSA Closely Involved in Guantanamo Interrogations, Documents Show, THE INTERCEPT (May 16, 2016); available at https://theintercept.com/2016/05/16/nsa-closely-involved-in-guantanamo-interrogations-documents-show/.

142 Margot Williams, Talya Cooper, and Micah Lee, NSA Used Porn to "Break Down Detainees" in Iraq – And Other Revelations from 297 Snowden Documents, THE INTERCEPT (March 1, 2018), available at https://theintercept.com/2018/03/01/iraq-porn-nsa-snowden-files-sidtoday/.

143 Jenna McLaughlin, How the U.S. Spies on Medical Nonprofits and Health Defenses Worldwide, THE INTERCEPT (Aug. 10, 2016), available at https://theintercept.com/2016/08/10/how-the-u-s-spies-on-medical-nonprofits-and-health-defenses-worldwide/.

144 Barton Gellman and Ashkan Soltani, NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden docu-ments say, WASHINGTON POST (October 30, 2013), available at https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

145 James Ball, NSA collects millions of text messages daily in 'untargeted' global sweep, THE GUARDIAN (Jan. 16, 2014), available at https://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep.

146 Spencer Ackerman and James Ball, Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ, THE GUARDIAN (Feb. 28, 2014), available at https://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo.

147 Margot Williams and Micah Lee, Iraqi Insurgents Stymied the NSA and Other Highlights from 263 Internal Agency Reports, THE INTERCEPT (Aug. 10, 2016), available at https://theintercept.com/2016/08/10/iraqi-insurgents-stymied-the-nsa-and-other-highlights-from-263-internal-agency-reports/.

148 Nick Turse, How the NSA Built a Secret Surveillance Network for Ethiopia, THE INTERCEPT (Sept. 13, 2017), available at https://theintercept.com/2017/09/13/nsa-ethiopia-surveillance-human-rights/.

149 Ryan Gallagher, NSA's Quiet Presence at a Base in England's Countryside Revealed in Snowden Documents, THE INTERCEPT (Sept. 13, 2017), https://theintercept.com/2017/09/13/digby-uk-nsa-gchq-surveillance/.

150 Id.

151 Williams and Lee supra note 147; and Ryan Gallagher, Inside Menwith Hill, THE INTERCEPT (Sept. 6, 2016), available at https://theintercept.com/2016/09/06/nsa-menwith-hill-targeted-killing-surveillance/.

152 Gallagher, supra note 149.

153 Glenn Greenwald, Laura Poitras, and Ewen MacAskill, NSA shares raw intelligence including Americans' data with Israel, THE GUARDIAN (Sept. 11, 2013), available at https://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents.

154 Henrik Moltke, Mission Creep: How the NSA's Game-Changing Targeting System Built for Iraq and Afghanistan Ended up on the Mexico Border, THE INTERCEPT (May 29, 2019), available at https://theintercept.com/2019/05/29/nsa-data-afghanistan-iraq-mexico-border/.

155 Von Spiegel Staff, The NSA's Secret Spy Hub in Berlin, SPIEGEL INTERNATIONAL (Oct. 27, 2013), available at https://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html.

156 Ryan Devereaux, Glenn Greenwald and Laura Poitras, The NSA is Recording Every Cell Phone Call in the Bahamas, THE INTERCEPT (May 19, 2014), available at https://theintercept.com/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/; Jacob Kastrenakes, The NSA is capturing nearly every phone call in Afghanistan, Wikileaks claims, THE VERGE (May 23, 2014), available at https://www.theverge.com/2014/5/23/5744616/nsa-capturing-nearly-all-afghanistan-phone-calls (citing WikiLeaks statement on the mass recording of Afghan telephone calls by the NSA, WIKILEAKS (May 23, 2014), available at https://wikileaks.org/WikiLeaks-statement-on-the-mass.html).

157 Julia Angwin and Jeff Larson, FAQ About NSA's Interest in Angry Birds and other 'Leaky Apps', PROPUBLICA (Jan. 28, 2014), available at https://www.propublica.org/article/faq-about-nsas-interest-in-angry-birds-and-other-leaky-apps.

158 For a full list of the spying programs disclosed by Snowden, see Snowden Revelations, LAWFARE, available at https://www.lawfareblog.com/snowden-revelations. See also Amos Toh, Faiza Patel, and Elizabeth Gotein, Overseas Sur-veillance in an Interconnected World, BRENNAN CENTER (2016) at 9, 39 for a discussion of the types of spying tactics used, how the limits on spying on U.S. persons were effectively circumvented, and which were justified under which authority.

159 Morgan Marquis-Boire, Glenn Greenwald, and Micah Lee, XKeyscore, THE INTERCEPT (July 1, 2015) available at https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/.

160 Toh, Patel and Gotein, supra note 158, and Sharon Goldberg, Surveillance without Borders: The "Traffic Shaping" Loophole and Why it Matters, CENTURY FOUNDATION (June 22, 2017) available at https://production-tcf.imgix.net/app/uploads/2017/06/03105333/surveillance-without-borders-the-traffic-shaping-loophole-and-why-it-matters.pdf .

161 Ryan Gallagher, NSA Blimp Spied in the United States, THE INTERCEPT (Apr. 24, 2017) available at https://theintercept.com/2017/04/24/nsa-blimp-spied-in-the-united-states/ .

162 Ryan Gallagher, NSA Kept Watch Over Democratic and Republican Conventions, Snowden Documents Reveal, THE INTERCEPT (Apr. 24, 2017) available at https://theintercept.com/2017/04/24/nsa-kept-watch-over-democrat-ic-and-republican-conventions-snowden-documents-reveal/ .

163 Office of the Inspector General, supra note 135.

164 Office of the Inspector General, A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006, (March 2008).

165 Office of the Inspector General of the U.S. Department of Justice, A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records, (Jan. 2010).

166 Id.; see also Doyle, supra note 136.

167 Notably, even with the broad reading of Section 215 created by the FISA Court ruling, the FBI, in at least some early cases, still violated the FISA Court's rulings where the Court ruled that an application for specific data under Section 215 violated the First Amendment. Office of the Inspector General of the U.S. Department of Justice, A Review of the FBI's Use of Section 215 Orders for Business Records in 2006, (March 2008).

168 For an in depth discussion on this program, see Privacy and Civil Liberties Oversight Board, Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court (January 23, 2014), available at https://fas.org/irp/offdocs/pclob-215.pdf .

169 Matthew Cole, The OPSEC Failures of Spies, BLACK HAT USA (Dec. 3, 2013), available at https://www.youtube.com/watch?v=BwGsr3SzCZc .

170 Privacy and Civil Liberties Oversight Board, supra note 168.

171 For an in-depth discussion on 702 and its abuses, see Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (July 2, 2014). Note, however, that although PCLOB provides an in-depth summary and explanation of the 702 program, its vindication of the legality of the program was widely challenged. See Spencer Ackerman, NSA reformers dismayed after privacy board vindicates surveillance dragnet, THE GUARDIAN (July 2, 2014), available at https://www.theguardian.com/world/2014/jul/02/nsa-surveillance-government-privacy-board-report . For more information on the 702 spying program, see also, Ashley Gorski and Patrick C. Toomey, Unprecedented and Unlawful: The NSA's "Upstream" Surveillance, JUST SECU-RITY (Sept. 19, 2016), available at https://www.justsecurity.org/33044/unprecedented-unlawful-nsas-upstream-sur-veillance/; and Jennifer Stisa Granick and Jadzia Butler, Correcting the Record on Section 702: A Prerequisite for Meaningful Surveillance Reform, JUST SECURITY (Sept. 15, 2016) available at https://www.justsecurity.org/32916/correcting-record-section-702-prerequisite-meaningful-surveillance-reform/; and Gotein and Patel, supra note 49.

172 Granick and Butler, Id., cites the Director of National Intelligence that 94,368 individuals were targeted under Section 702 in 2015.

173 Ryan Gallagher and Henrik Moltke, The Wiretap Rooms, THE INTERCEPT (June 25, 2018) available at https://theintercept.com/2018/06/25/att-internet-nsa-spy-hubs/.

174 Memorandum Opinion, Bates (FISA Ct. Oct. 3, 2011) (hereinafter "The Bates Opinion"). See also Benjamin Wittes and Lauren Bateman, The NSA Documents, Part II: The October 2011 FISC Opinion, LAWFARE (Aug. 22, 2013), available at https://www.lawfareblog.com/nsa-documents-part-ii-october-2011-fisc-opinion .

175 The Bates Opinion, Id.

176 Privacy and Civil Liberties Oversight Board, supra note 171.

177 Siobhan Gorman, NSA Officers Spy on Love Interests, WALL STREET JOURNAL (Aug. 23, 2013).

178 See generally, Jerome P. Bjelopera, Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative: Background and Issues for Congress, CONGRESSIONAL RESEARCH SERVICE (2011).

179 See generally, Michael Price, National Security and Local Police, BRENNAN CENTER (2013).

180 Staff of the S. Permanent Subcomm. On Investigations, 112th Congress, Federal Support for and Involvement in State and Local Fusion Centers, 26-45, 57, 67, 83.

181 USA Freedom Act, PUB. L. NO. 114-23 (2015).

182 Elizabeth Gotein, Reauthorizing the USA Freedom Act of 2015, BRENNAN CENTER (Nov. 6, 2019); Faiza Patel and Raya Koreh, Enhancing Civil Liberties Protections in Surveillance Law, BRENNAN CENTER (Feb. 27, 2020).

183 Sean D. Carberry, NSA halts Section 702 'upstream' collection, FCW (Apr. 28, 2017) available at https://fcw.com/articles/2017/04/28/702-upstream-nsa-carberry.aspx.

184 See, e.g. Benjamin Wittes, The President's Speech and PPD-28: A Guide for the Perplexed, LAWFARE (Jan. 20, 2014) available at https://www.lawfareblog.com/presidents-speech-and-ppd-28-guide-perplexed.

185 Jenna McLaughlin, The U.S. Government's Privacy Watchdog is Basically Dead, Emails Reveal, THE INTERCEPT (March 3, 2017) available at https://theintercept.com/2017/03/03/the-governments-privacy-watchdog-is-basically-dead-emails-reveal/.

186 Glenn Greenwald and Murtaza Hussain, Meet the Muslim-American Leaders the FBI and NSA have been Spying on, THE INTERCEPT (July 9, 2014), available at https://theintercept.com/2014/07/09/under-surveillance/.

187 Jana Winter & Sharon Weinberger, The FBI's New U.S. Terrorist Threat: 'Black Identity Extremists', FOREIGN POLICY (Oct. 6, 2017).

188 Alice Speri, The FBI Spends a Lot of Time Spying on Black Americans, THE INTERCEPT (Oct. 29, 2019).

189 Department of Justice, Attorney General William P. Barr's Statement on Riots and Domestic Terrorism (May 31, 2020).

190 Mark Hosenball, U.S. Congress pushing Homeland Security for Details on Protest Surveillance, ASSOCIATED PRESS (28 July, 2020).

191 Trevor Aaronson, FBI's "Hamas" Sting Against Boogaloo Boys Was So Absurd that Even Hamas Spoke Out Against It, THE INTERCEPT (Sep. 20, 2020).

192 Department of Homeland Security, United States Begins Implementation of Changes to the Visa Waiver Program (Jan. 21, 2016); Department of Homeland Security, DHS Announces Further Travel Restrictions for the Visa Waiver Program (Feb. 18, 2016).

193 Trump v. Hawaii, 585 U.S. ¬¬¬_____ (2018).

194 National Immigration Law Center, Understanding Trump's Muslim Bans (2019). For a discussion on how the Muslim Ban and "extreme vetting" has undermined the rights and safety of Muslim refugees and devastated their families, see International Refugee Assistance Project, Debunking "Extreme Vetting": Recommendations to Build Back the U.S. Refugee Admissions Program (October 2020).

195 Nicole Narea, House Democrats just passed a bill to repeal Trump's travel bans, VOX (July 22, 2020) available at https://www.vox.com/2020/7/22/21332511/no-ban-act-travel-ban-bill-trump.

196 The White House, Proclamation on Ending Discriminatory Bans on Entry to the United States, (Jan. 20, 2021) available at https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/20/proclamation-ending-discriminatory-bans-on-entry-to-the-united-states/.

197 Ryan Devereaux, Homeland Security Used a Private Intelligence Firm to Monitor Family Separation Protests, THE INTERCEPT (Apr. 29, 2019).

198 Ryan Devereaux, Journalists, Lawyers, and Activists Working on the Border Face Coordinated Harassment from U.S. and Mexican Authorities, THE INTERCEPT (Feb. 8, 2019).

199 Carberry, supra note 183.

200 Sharon Bradford Franklin, Fulfilling the Promise of the USA Freedom Act: Time to Truly End Bulk Collection of Americans' Calling Records, JUST SECURITY (Mar. 28, 2019).

201 Charlotte Butash and Margaret Taylor, What's in H.R. 6172, the House's Compromise FISA Reform Bill? LAWFARE (March 11, 2020).

202 Id.

203 Margaret Taylor, The Specter of FISA Reform Haunts Capitol Hill, LAWFARE (May 29, 2020).

204 For a discussion on how First Amendment arguments from some of these other cases might be creatively distinguished and exercised in surveillance cases, see Matthew A. Wasserman, First Amendment Limitations on Police Surveillance: The Case of the Muslim Surveillance Program, 90 N.Y.U. L. Rev. 1786 (2015).

205 Jeffrey L. Vagle, Laird v. Tatum and Article III Standing in Surveillance Cases, 18 U. PA. J. CONST. L. 1055. See also Chapter 1, citing Church Committee Report Book 3 at 800-804.

206 In ACLU v. Clapper, 785 F.3d 787 (2d Cir. 2015), the Second Circuit hinted that similar concerns might apply to overbroad NSA bulk metadata collection, before resolving the case on narrower grounds.

207 Such claims are known as "Bivens" suits after Bivens v. Six Unknown Named Agents, 403 U.S. 388 (1971) which found standing for an individual to sue federal agents for constitutional violations absent an explicit statutory grant.

208 ACLU v. Clapper, 785 F.3d 787 (2d Cir. 2015) also strongly suggested that the Smith rule may no longer be valid given the drastic technological changes that have taken place since. The Court nonetheless refused to make such a holding and resolved the case on statutory grounds. The report by the Privacy and Civil Liberties Oversight Board into the NSA's CDR program, supra note 169 at 112-114, also emphasizes that the Third Party Doctrine may no longer be applicable in the context of mass metadata collection and that many state high courts have rejected its application in specific circumstances. At the time of writing, a defendant in a criminal case is challenging the use of geolocation data obtained from his passive use of various Google services on his smartphone that were obtained via a subpoena. U.S. v. Chatrie, 3:19-cr-00130 (E.D. Va. 2020). For a discussion about what cell phone information can be obtained by whom, see Citizen Lab, The Many Identifiers in Our Pockets: A Primer on Mobile Privacy and Security, (May 21, 2015), available at https://citizenlab.ca/2015/05/the-many-identifiers-in-our-pocket-a-primer-on-mobile-privacy-and-security/.

209 The men's First Amendment claim failed on strict scrutiny grounds for similar reasons where the court held that a border search was the "least intrusive" means. Id. at 102-105.

210 Though torture is an extreme form of surveillance abuse, the primary areas of law under which torture claims under the "War on Terrorism" have been litigated are the Alien Tort Statute and the Torture Victims Protection Act. Such claims focus on the brutality and indignity of the methods rather than the scope of information that the government is permitted to obtain and why. As such, an extended discussion of these areas of law is not included in this report. For a primer on relevant law, see David Nersessian, International Human Rights Litigation: A Guide for Judges, FEDER-AL JUDICIAL CENTER (2016) available at https://www.fjc.gov/sites/default/files/2017/Intl_Human_Rights_Litigation_2017.pdf.

211 See Donner, supra note 16.

212 Georgia Bureau of Investigation, Directive 7-6 (Feb. 15, 2018) at 4.

213 Id. at 5.

214 Id. at 10.

215 National Suspicious Activity Reporting Initiative, Indicators and Behaviors, available at https://www.dhs.gov/sites/default/files/publications/16_0208_NSI_SAR-Indicators-Behaviors-Tools-Analysts-Investigators.pdf.

216 Georgia Bureau of Investigation, supra note 212 at 15.

217 Id. at 16.

218 Georgia Bureau of Investigation, Directive 8-6-5 (Oct. 26, 2012) at 3-4.

219 Id. at 7.

220 Id. at 9.

221 Id. at 10.

222 Georgia Bureau of Investigation, Directive 8-8-23 (Jan. 27, 2017) at 1.

223 Id.

224 Id. at 2.

225 Id. at 3.

226 ACLU, No Real Threat: The Pentagon's Secret Database on Peaceful Protest (2007).

227 ACLU, School of the Americas Watch – FBI/JTTF Documents Released (2006), available at https://www.aclu.org/other/school-americas-watch-fbijttf-documents-released?redirect=cpredirect/25436. The School of the Americas is now known as the Western Hemisphere Institute for Security Cooperation.

228 For background about and criticism of this investigation, see Canadian Coalition for Peace and Justice, Submission to the United Nations Human Rights Council Fourth Universal Periodic Review – Canada (2008), Office of the High Commissioner of Human Rights (2008), available at https://lib.ohchr.org/HRBodies/UPR/Documents/Session4/CA/CCPJ_CAN_UPR_S4_2009_CanadianCoalitionforPeaceandJustice.pdf.

229 In the prosecution of Ahmed, the prosecutor surmised: "The case before you is not about throwing bombs and shooting soldiers" before discussing the conspiracy and material support charges. Transcript of Proceedings at 878, United States v. Ahmed, No. 1:06-CR-147-WSD-1 (N.D.G.A 2009). Similarly, the prosecutor stated in Sadequee's prosecution: " It's…not a case about actual acts of terrorism…you didn't see any bombs go off " before discussing the vague and confusing differences between acts of speech and conspiracy, attempt, and material support crimes. Transcript of Proceedings at 1359, United States v. Sadequee, No. 1:06-CR-147-WSD-2 (N.D.G.A. 2009).

230 Transcript of Sadequee, Id. at 1371.

231 Transcript of Ahmed, supra note 229 at 887.

232 Transcript of Sadequee, supra note 229 at 1396.

233 Murtaza Hussain, New Film Delves into FBI Arrests of Youths for Terrorism Crimes They Might Commit, THE INTERCEPT (Mar. 6, 2016).

234 Aviva Stahl, Why Are Queer Activists and Muslim Scholars Holding Vigils Outside a Manhattan Prison?, THE NATION (May 30, 2014) (citing comments from United Nations Special Rapporteur Juan Mendez that "[Solitary confinement] in pre-trial detention is particularly objectionable because the pain and suffering of a mental or psychological nature that the person suffers prepares him psychologically to either confess or make statements against his interests, or even plead guilty…It seems to me that in terrorism cases, at least, that's a very deliberate policy of the United States.").

235 N.C.G.S. § 132-1.4.

236 N.C.G.S § 132-1.4, 1.7.

237 Jane Porter, How Local Law Enforcement Spies on Citizens, INDYWEEK (Feb. 11, 2015).

238 Trevor Aaronson, Trial & Terror: North Carolina, THE INTERCEPT, available at https://trial-and-terror.theintercept.com/people/.

239 State Bureau of Investigation, North Carolina Information Sharing & Analysis Center Procedure Manual (2017) at 28-29.

240 Id. at 10.

241 Id. at 29-30, 34.

242 Ryan Devereaux, Homeland Security Sees Anger At Trump as a Driver of "Domestic Terrorist Violence", THE INTERCEPT (Mar. 2, 2017).

243 Michael Schwalbe, UNC Police Spying Threatens Free Speech, THE NEWS & OBSERVER (Nov. 15, 2017).

244 Michael Biesecker, Plain-Clothes Officer Attended Moral Monday Planning Meetings, ASSOCIATED PRESS (Oct. 7 2013).

245 See Aaronson, supra note 238.

246 Department of Justice Office of Public Affairs, Seven Charged with Terrorism Violations in North Carolina, (July 27, 2009) available at https://www.justice.gov/opa/pr/seven-charged-terrorism-violations-north-carolina; Department of Justice -- U.S. Attorney's Office, Eastern District of North Carolina, Fourth Circuit Affirms Convictions of Boyd Defendants, (Feb. 14, 2014) available at https://www.justice.gov/usao-ednc/pr/fourth-circuit-affirms-convictions-boyd-defendants.

247 Memorandum of Law in Support of 28 U.S.C. § 2255 Habeas Petition, Yaghi v. United States, No: 5:09-cr-00216-FL (E.D.N.Y. 2016), available at https://mlfa.org/news/attorneys-challenge-unconstitutional-conviction-of-ziyad-yaghi/.

248 Id.

249 United States v. Hassan, 742 F.3d 104, 137-139 (4th Cir. 2014).

250 Trevor Aaronson, Trial & Terror: Florida, THE INTERCEPT, available at https://trial-and-terror.theintercept.com/people/.

251 Joshua Ceballos, UM Used Surveillance to Track Student Protesters, MIAMI NEW TIMES (Oct. 15, 2020).

252 Miami Dade Police Department, Southeast Florida Fusion Center Privacy Policy Ver. 3.1 (May 2015) at 3.

253 Id. at 6; Florida Fusion Center, Privacy Policy Ver. 3.2 at 5.

254 Miami-Dade Police Department, supra note 252 at 6-7; Florida Fusion Center, Id. at 5.

255 Id. at 7; Florida Fusion Center, supra note 253 at 5.

256 Id.

257 Linda Trischitta, Police Show Off Homeland Security Intelligence Center, SUN-SENTINAL (Mar. 20, 2015).

258 Terrence McCoy, Raees Qazi: Accused Terrorist's Real Story, MIAMI NEW TIMES (Dec. 27, 2012).

259 Richard B. Schmitt, The Patriot Act Can't Make Up for a Weak Case, L.A. TIMES (Dec. 8, 2005).

260 American Association of University Professors, Academic Freedom and Tenure: University of South Florida, ACADEME (May-June 2003).

261 Id.

262 USF Fires Indicted Professor, ASSOCIATED PRESS (Feb. 27, 2003).

263 Department of Justice, Members of the Palestinian Islamic Jihad Arrested, Charged with Racketeering and Conspiracy to Provide Support to Terrorists (Feb. 20, 2003).

264 Amnesty International, USA: Amnesty International Raises Concern About Prison Conditions of Dr. Sami Al-Arian (29 July 2003), available at https://www.amnesty.org/en/documents/AMR51/110/2003/en/.

265 Murtaza Hussain and Glenn Greenwald, Exclusive Interview: Sami Al-Arian, Professor Who Defeated Controversial Terrorism Charges, Is Deported From U.S., THE INTERCEPT (Feb. 5, 2015).

266 Id.

267 Department of Justice, Seven Florida Men Charged with Conspiring to Support al Qaeda, Attack Targets in the United States (June 23, 2006).

268 Factbox: Miami Terrorism Trial of Liberty City Seven, REUTERS (Dec. 13, 2007).

269 Trevor Aaronson, The Released: Part 1, THE INTERCEPT (Apr. 20, 2017).

270 Louisiana State Analytical & Fusion Exchange, Privacy Policy (Mar. 19, 2019) at 4-5.

271 Id. at 5.

272 Id.

273 South Carolina Law Enforcement Division, SC Information and Intelligence Center: Privacy, Civil Rights, and Civil Liberties Protection Policy at 4.

274 Id. at 30.

275 City of Charleston Police Department, Policy & Procedure Manual: General Order 8.2 (Apr. 6, 2018).

276 City of Charleston Police Department, Policy & Procedure Manual: General Order 37 (Feb. 1, 2017).

277 For a detailed analysis of the shortcomings of this litigation victory, see Fazaga v. FBI, Ninth Circuit Holds that FISA Displaces the State Secrets Privilege for Electronic Surveillance, 133 HARV. L. REV. 1774 (2020).

278 Stipulation of the Settlement at 3, Hassan v. City of New York, 804 F.3d 277 (3d Cir. 2015) (discussing the relevance of the Handschu guidelines to the settlement agreement).

279 J. David Goodman, New York City Council Votes to Increase Oversight of Police Dept., NEW YORK TIMES, June 27, 2013.

280 Though it has not been introduced by any members of Congress, the Entrapment Governmental Overreach (EGO) Bill has been written and put forward to the offices of a number of members of Congress by the Coalition for Civil Freedoms, an organization set up by the family and friends of Dr. Sami Al-Arian, discussed in chapter 2, to provide services and advocacy to families of persons convicted under overbroad counter-terrorism statutes. The bill would require federal prosecutors to establish the pre-existence of a criminal conspiracy when trying criminal cases involving informants.

281 Examples of this phenomenon include reporting on some of the original Snowden leaks which focused on the NSA spying on prominent Muslims, and terrorism databases that overwhelmingly focused on Arab-Americans. This is discussed in Kumar & Kundnani, supra note 10.

282 A July 2017 poll indicates that nearly 4 in 10 Americans believe it is justifiable for law enforcement to profile Arab-Americans or Muslim-Americans. Arab American Institute, American Attitudes: Immigration, Civil Rights, Surveillance, Profiling, and Hate Crimes (July 2017).

283 Details of the campaign in Kenner are based on a telephone interview with Sabrine Mohamed, an attendee of the mosque and a local activist on Apr. 7, 2020.

284 Telephone interview with Celine Qussiny of Palestinian Youth Movement and Nadia Guzman of Stop LAPD Spying (April 9, 2020).

285 An anti-CVE toolkit containing these resources is available at https://msawest.org/resources/.

286 Id.

287 Letter from Randi Weingarten, President, American Federation of Teachers, to James B. Comey, Director, FBI (Aug. 9, 2016).

288 Letter from Alex Caputo-Pearl, President, UTLA, to whom it may concern (July 23, 2018).

289 See Second Amended Complaint, CAIR v. DHS (Case No. 2:17-cv-07887-PSG-KS) (C.D.C.A 2018) (discussing all information requests, exhausted remedies, and basis of litigation under FOIA).

290 Deepa Bharath, LA mayor turns down $425K in federal funding to counter violent extremism after opposition from civil rights groups stalls process, ORANGE COUNTY REGISTER (Aug. 16, 2018).

291 A detailed history behind the MOU is found in Section 1 of an unenacted version of the San Francisco Civil Rights Ordinance, available at https://www.sfbos.org/ftp/uploadedfiles/bdsupvrs/committees/materials/ps120046tdr.pdf.

292 Id.

293 San Francisco Human Rights Commission, Community Concerns of Surveillance, Racial and Religious Profiling of Arab, Middle Eastern, Muslim, and South Asian Communities and Potential Reactivation of SFPD Intelligence Gathering, 15 (Sept. 23, 2010).

294 Id.

295 Maria L. La Ganga, FBI Documents reveal profiling of N. California Muslims, L.A. TIMES (Mar. 28, 2012) (describing both the lawsuit and records requests pertaining to spying).

296 San Francisco Human Rights Commission, supra note 293.

297 Arab Resource & Organizing Center, Proposed Law Would Restore Local Control Over Intelligence Gathering (Jan 25, 2012), available at http://araborganizing.org/proposed-law-would-restore-local-control-over-intelligence-gathering/.

298 Arab Resource & Organizing Center, Hundreds Rally and Pray Jumaa Outside Civic Center to Support Ordinance, (Mar. 30, 2012), available at http://araborganizing.org/actionalerts/hundreds-rally-and-pray-jumaa-outside-civic-center-to-support-ordinance.

299 Sarah Medina, Safe San Francisco Civil Rights Ordinance: Landmark Law Requires Community Input on Police Cooperation with FBI, HUFFINGTON POST (May 10, 2012).

300 San Francisco, Cal., Ordinance 83-12 (May 9, 2012).

301 Alex Emslie and Mina Kim, Complaint Alleges SFPD Officer Broke City Law While Investigating with FBI, KQED (Mar. 26, 2015) available at: https://www.kqed.org/news/10465873/complaint-alleges-sfpd-officer-broke-city-law-while-investigating-with-fbi; and Nasrina Bargzie, Safe San Francisco Civil Rights Ordinance: Third Year Report, ASIAN AMERICANS ADVANCING JUSTICE – ASIAN LAW CAUCUS (Feb. 11, 2015), available at https://www.advancingjus-tice-alc.org/news_and_media/safe-san-francisco-civil-rights-ordinance-third-year-report/.

302 Ryan Devereaux, FBI and San Francisco Police Have Been Lying About Scope of Joint Counterterrorism Investigations, Document Suggests, THE INTERCEPT (Nov. 1, 2019).

303 Katie Utehs, San Francisco temporarily suspends ties to FBI joint terrorism task force, ABC 7 NEWS (Feb 2, 2017) available at https://abc7news.com/news/sf-temporarily-suspends-ties-to-fbi-joint-terrorism-task-force/1733119/.

304 Anna Sciacca, Oakland withdraws police from FBI joint terrorism task force, SAN JOSE MERCURY NEWS (Oct. 21, 2020).

305 For a detailed description of the bill as it was originally written, see Project South, SB 15 Threatens the Safety of Georgia's Students of Color, available at https://projectsouth.org/wp-content/uploads/2019/02/SB-15-Fact-Sheet.pdf.

306 Id.

307 Ty Tagami, Georgia Legislature passes school security bill, ATLANTA JOURNAL-CONSTITUTION (Apr. 3, 2019).

308 Id. Project South continued to express concern. See Project South, SB 15 Threatens the Safety of Georgia's Students of Color (Updated), available at https://projectsouth.org/wp-content/uploads/2019/04/4.14-SB-15-Final-Updated-Fact-Sheet.pdf?fbclid=IwAR2niT-VI4gxdHwBUeGVWFs0cVKDA4i4lDmRtZmlQ_et2ig312dsGxqgEOKc.